Reference Architecture

Version 5.0 – 13/06/2018

Table of Contents

Table of Figures

Introduction

This reference architecture contains a set of structures, patterns and guidelines describing how IT systems should be built across the organization. It also provides a common vocabulary with which to discuss implementations, with the aim to stress reusability and commonality.

This document serves the basis for concrete solution architectures. The goal of this template is the harmonisation of IT solutions across the organisation and the reusability of them increasing the agility in building them. It also aims to ease the adaptability of these solutions to other scenarios, like integrating future changes or adopting them by our partners.

OVERVIEW

During the last years EUIPO has growth in a fast pace, the IT solutions has been developed with tight deadlines.

This has resulted in a quite organic architecture of our applications landscape. Nowadays we have some tightly coupled applications quite difficult to adapt without impacting others. At Infrastructure level we have a similar scenario, where the different elements have been put in place according to short-term priorities, and normal operational tasks are performed based on best-effort initiatives.

A global map of how everything fits together and what the target architecture is has not been put in place.

A Reference Architecture was developed in 2012 by the Architecture Service in the scope of the CF programme, covering the needs of the projects inside the programme. The CF Reference Architecture has been shown its convenience and utility for the implementation of the tools and the installation and configuration of the different operation services required to support the tools. CF programme was selected for this initiative because it was a Greenfield scenario with a main focus in building solutions for sharing with other partners. For that reason, there was an opportunity of proposing some improvements and bringing in place new models without compromising any of the existing services and infrastructure.

Based on the success of this initiative and the positive feedback received, the Reference Architecture for EUIPO is described in the following document. It serves as a map of what our legacy systems look like and what are the target technologies and products.

The version 1.0 developed in 2013 established a common technological framework for applications developed under the scope of EUIPO or CF programme. EUIPO Infrastructure is also covered in this document. The infrastructure available in each National Office participating in the CF programme is outside the scope of this document.

Our Architecture will follow a Service Oriented approach and Software and Infrastructure will be provisioned and developed as Services.

ASSUMPTIONS

- Only major versions will be described in this document, minor versions are not mentioned in this document, as according to the best practices in the market, they contain functionality and security fixes that respect backward compatibility with the major versions.
- Minor versions shall be applied to the environments at regular basis. Minor versions containing security or stability patches shall be applied ASAP, in case this could be not fulfilled a maximum periodicity of 3 months shall apply, minor versions containing only functionality fixes shall be applied every 6 months. The patches shall be applied to the environments in the following order: Development & Integration, Test & Preproduction and finally Production. In order to promote the patches from one environment to the following environment a set of regression and stability tests shall be performed. These tests shall be defined and automated.
- As EUIPO shall be a mainstream adopter regarding Technology, no new product or technology or a major version of a product which is less than 6 months old shall be installed or used in production.
- New projects willing to adopt a new major version of one product in the catalogue could start using it in development when that version has been at least 3 months in the market.
- New products or technologies which are not in the catalogue shall not be used unless an exception is granted by Architecture. When a new product will be considered to be part of the reference, it will be added into the new issues of this document.
- The set of technologies and products described in this document is a reference for new in-house developments, but it shall not affect the adoption of a COTS suite or products which are bought. For example, if we buy a product which is implementing an old version of Java, or is used internally a DB or a Search engine, which is obsolete or newer that the ones described in this document, it is completely accepted the usage of this version or product, as it constitutes an intrinsic part of the purchased COTS product. No development shall be done to modify to perform any modification on these products.

HOW TO READ IT

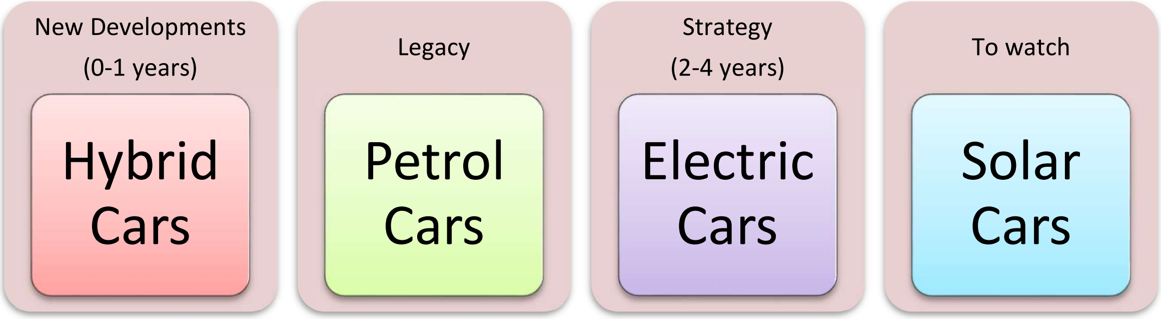
The reader of this RA can read it from beginning to the end or can skip some areas to focus on the topic more interesting to him/her.

The RA defines what products or technologies can be used for new projects starting during this and next year, this is described in the column titled “New Developments”.

It also describes which products and technologies are currently supported because there are legacy systems which are under maintenance, the column for this is “Legacy”. Only projects related to maintenance of systems are allowed to continue using these technologies, and only if the cost of migrating to the newer one is bigger than the cost of the technical debt created by using this old technology (Cost of extended or end-of-life support, and the cost of recruiting resources with these skills should be considered)

The products and technologies to be used in the near future (next 2 to 4 years) are described in “Strategy”.

In “To watch” column technologies that are interesting to be watched and could be considered in the future but at the moment of writing this document, there are no plans for adopting them.



New Developments (0-1 years)	Legacy	Strategy (2-4 years)	To watch
Hybrid Cars	Petrol Cars	Electric Cars	Solar Cars

REFERENCES

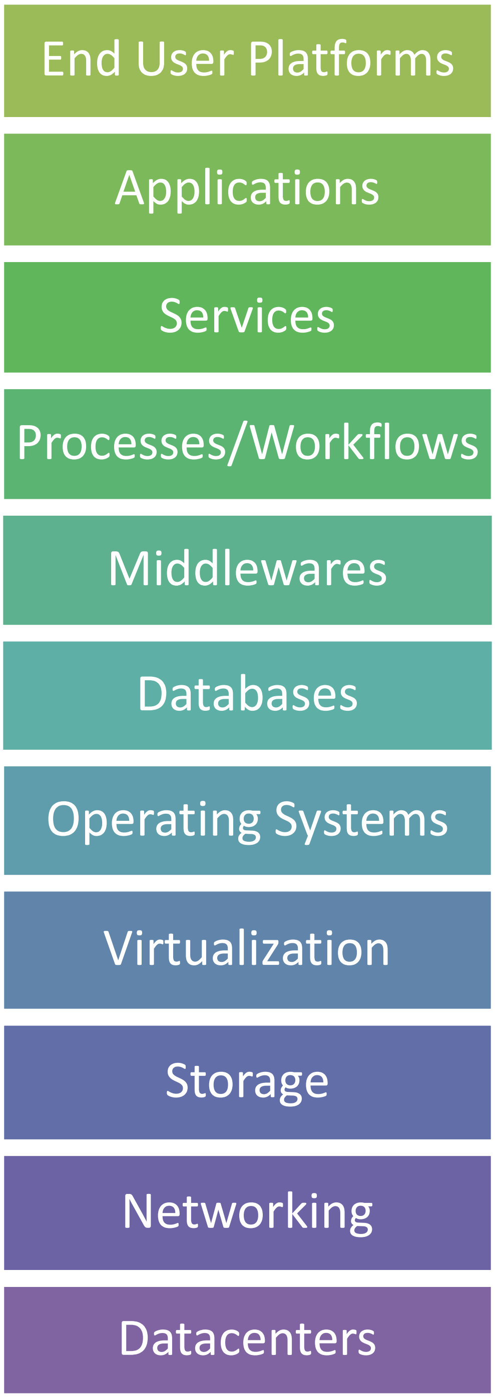
Ref.	Version	Location
[R1]	1.5	EUIPO IT Standards
[R2]		
[R3]		
[R4]		
[R5]		

TERMS, ACRONYMS AND ABBREVIATIONS

Term	Location
SSO	Single Sign On
GUI	Graphical User Interface
RA	Reference Architecture
FF	Firefox
FF ESR	Firefox Extended Support Release
IE	Internet Explorer

1 Areas of concerns

The following graphic describes the areas or concerns to be covered in this Reference Architecture (RA from now on)



End User Platforms

Applications

Services

Processes/Workflows

Middlewares

Databases

Operating Systems

Virtualization

Storage

Networking

Datacenters

2 End User Platforms

In this area the Browsers, Operating Systems and Mobile Devices supported by IT will be described.

We will distinguish between Internal and External users, as the difference in the homogeneity of platforms to be supported, differs greatly.

2.1 INTERNAL USERS

Our internal customers use homogenous platforms delivered by the office, therefore is a much more controlled environment.

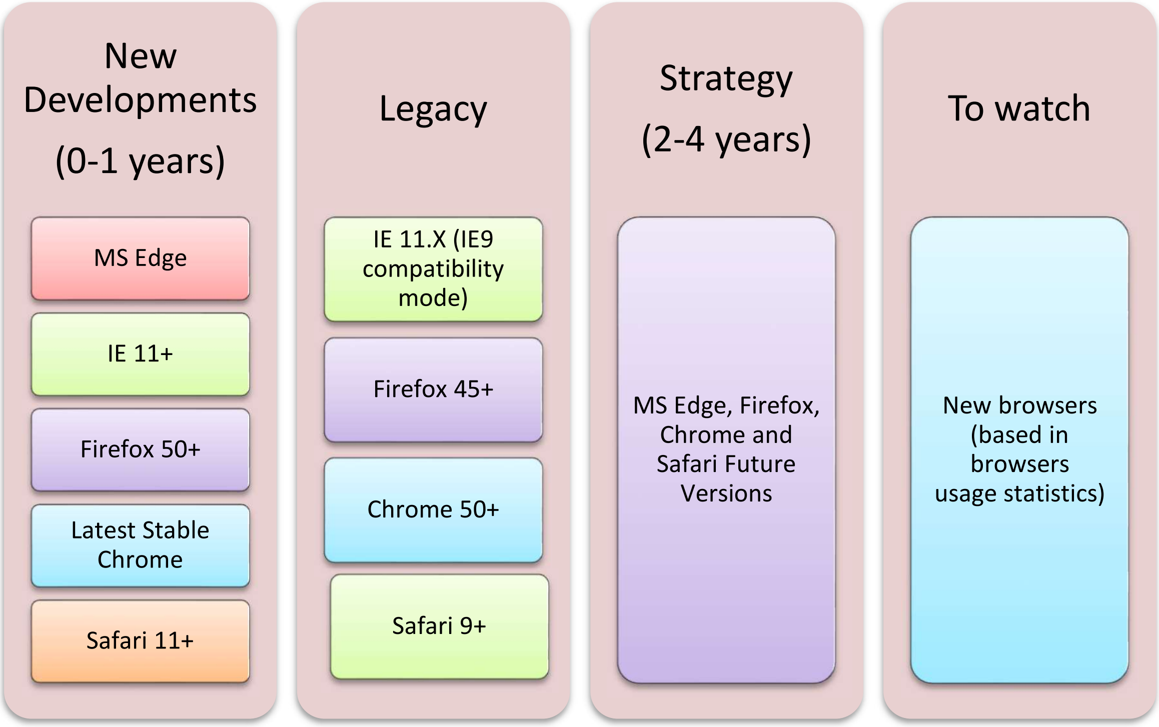
At the moment of writing this version of the RA, the new devices delivered to the users at the office have the following configuration:

PCs with Windows 10 OS, Microsoft Office 2016, IE 11.x, FF ESR 52.x, Chrome 63.x

2.1.1 Browsers

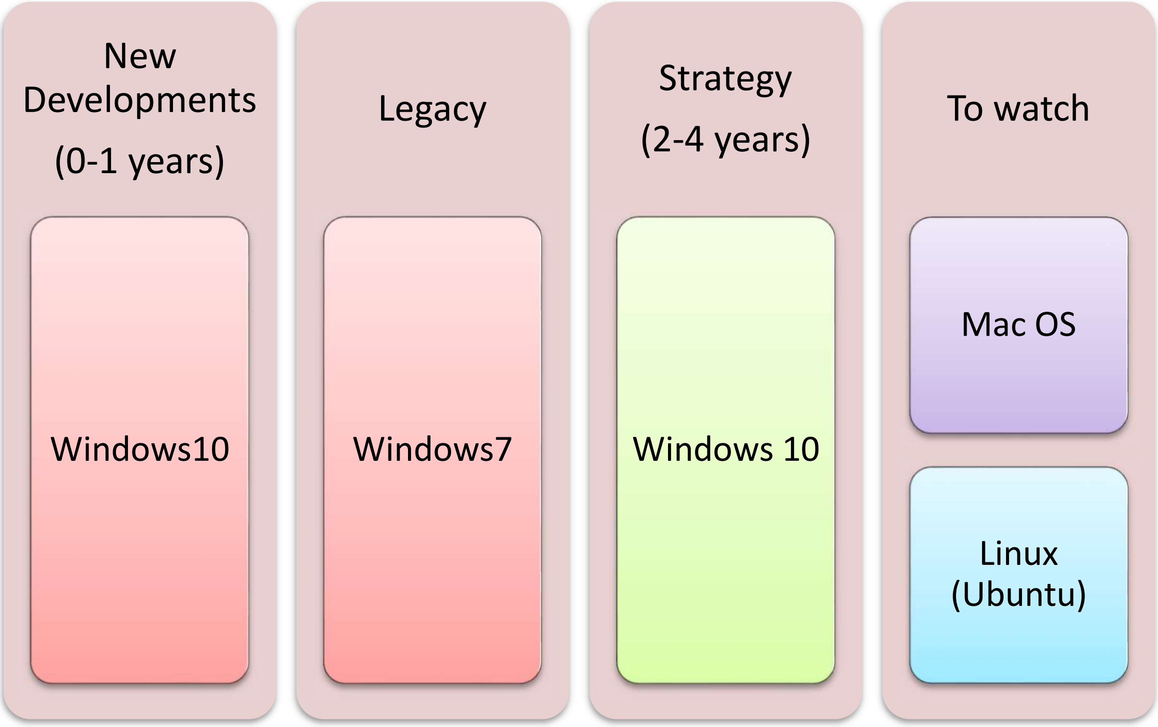
In order to be able to decommission and update the old browsers, we will require that every new project is tested against the browsers in the "New Development" column. Legacy systems will maintain backward compatibility with the browser versions specified in the "Legacy" column but it is recommended to do a technical upgrade to make them compatible with the new versions ("New Development").

As there are more employees using mobile devices, web applications should be responsive and should provide a nice user experience even using those devices. Applications should be prepared for displaying in high resolution devices.



New Developments (0-1 years)	Legacy	Strategy (2-4 years)	To watch
MS Edge	IE 11.X (IE9 compatibility mode)	MS Edge, Firefox, Chrome and Safari Future Versions	New browsers (based in browsers usage statistics)
IE 11+	Firefox 45+		
Firefox 50+	Chrome 50+		
Latest Stable Chrome	Safari 9+		
Safari 11+			

2.1.2 Operating Systems



New Developments (0-1 years)

Windows10

Legacy

Windows7

Strategy (2-4 years)

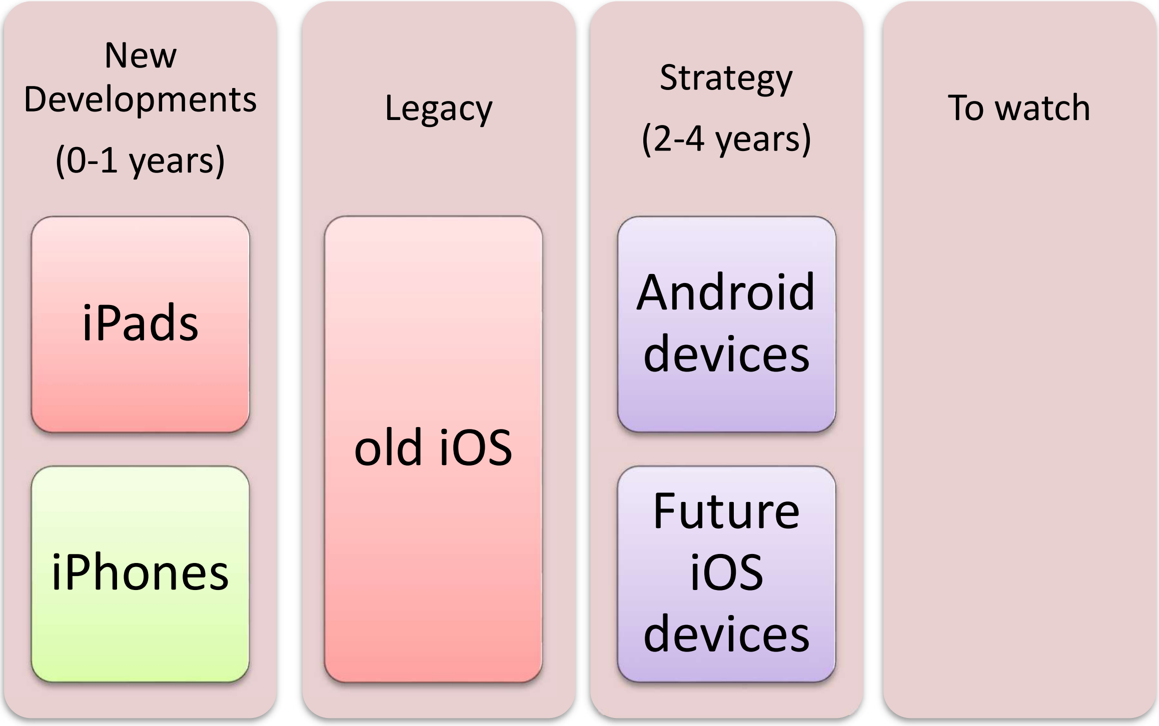
Windows 10

To watch

Mac OS

Linux (Ubuntu)

2.1.3 Mobile Devices

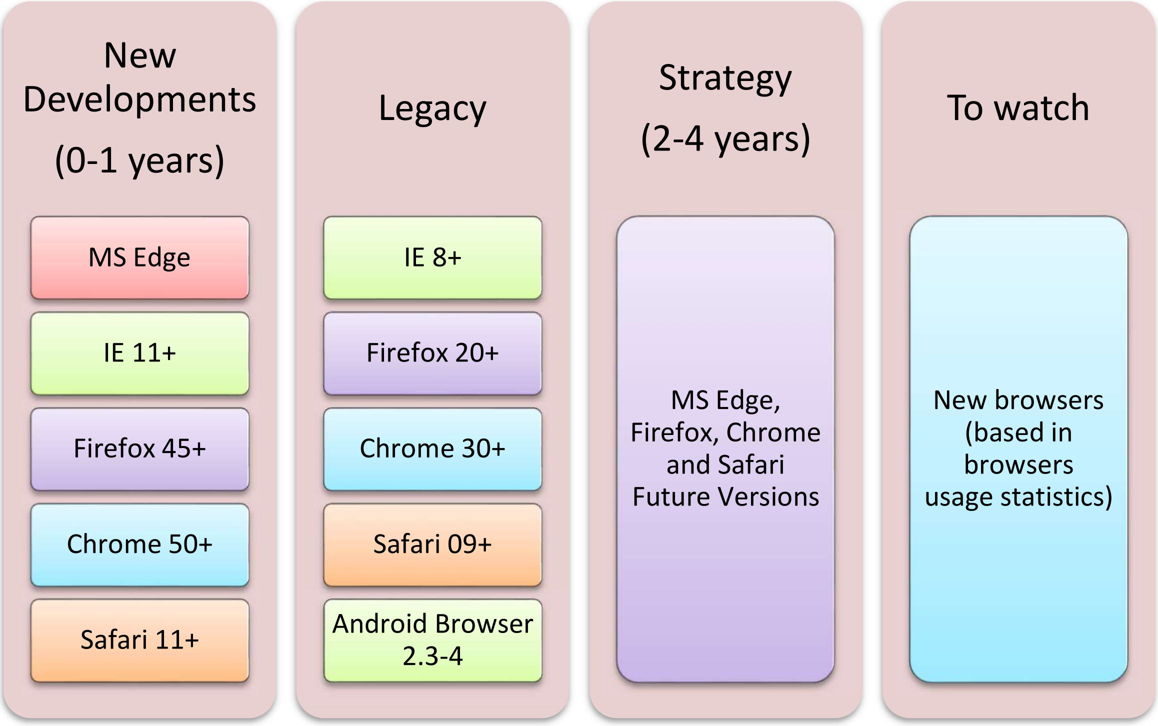


2.2 EXTERNAL USERS

Our external customers use heterogeneous platforms that the ones managed by the office, therefore the number of technologies and products to be provided/supported is bigger.

External customers' technologies support supposes a very broad scope, as some of our customers use the latest devices and technologies while others do not update technology very often. The pace to update this chapter will be a little bit slower that the internal users one.

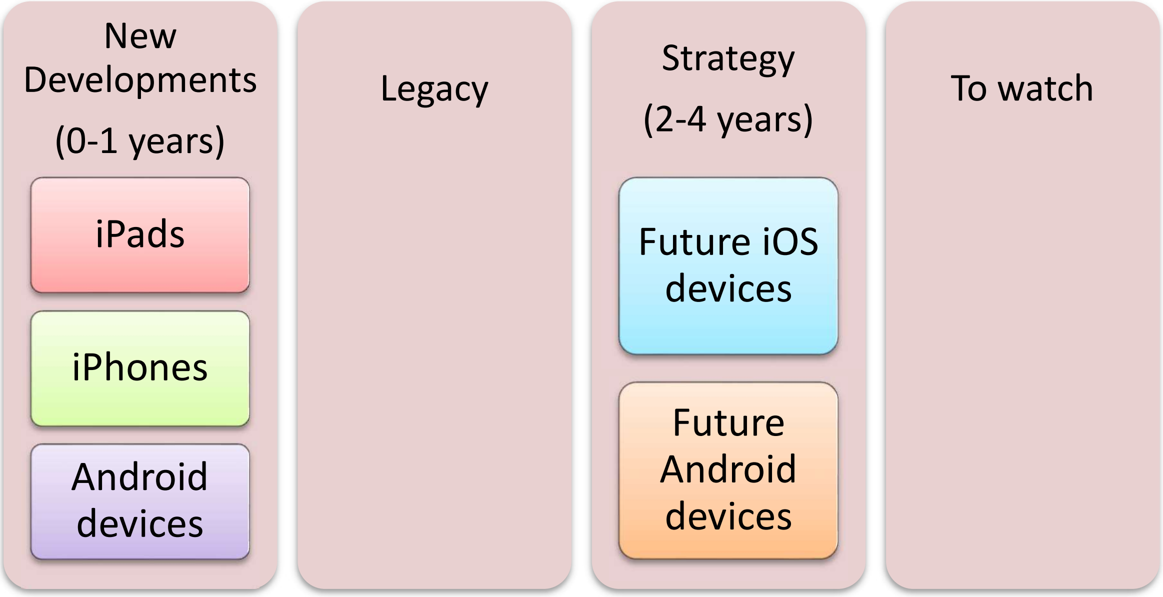
2.2.1 Browsers



New Developments (0-1 years)	Legacy	Strategy (2-4 years)	To watch
MS Edge IE 11+ Firefox 45+ Chrome 50+ Safari 11+	IE 8+ Firefox 20+ Chrome 30+ Safari 09+ Android Browser 2.3-4	MS Edge, Firefox, Chrome and Safari Future Versions	New browsers (based in browsers usage statistics)

2.2.2 Mobile Devices

External Applications should be prepared for displaying in different types of mobile devices including high resolution devices as Retina display based.



New Developments (0-1 years)	Legacy	Strategy (2-4 years)	To watch
iPads iPhones Android devices		Future iOS devices Future Android devices	

3 Applications

At the time of designing new systems and applications, a principle about simplicity shall apply. This means not to use complex architectures when the system does not require it. Therefore, when possible do not use other libraries for implementing the same services that are already delivered by the Application or Web Server itself.

Do not complicate your architecture using frameworks if the framework is not well-known by the resources assigned to the implementation of the application.

Your customer does not care if the bug is in a library, in a framework or in a third party tool you have selected for implementing the application. As soon as you adopted it, it is part of the application, and if it fails, your application fails. Therefore, do not use a library or other product if your team do not have enough experience with it or it is not really needed, as the defects of the tool can be inherit on your system.

On the other hand, if the library, framework or tool is well-known and established in the market, it is preferred to reuse something already tested that do in-house new development which needs to be tested.

Under these premises, our recommendation will be to follow a Spring Boot (Tomcat- based) architecture if no extra JEE services are required. If using Tomcat with Spring fulfils your needs, keep it simple. Use a JEE Application Server as JBoss in case JEE services, as EJBs, JPA, JTA, etc… are required.

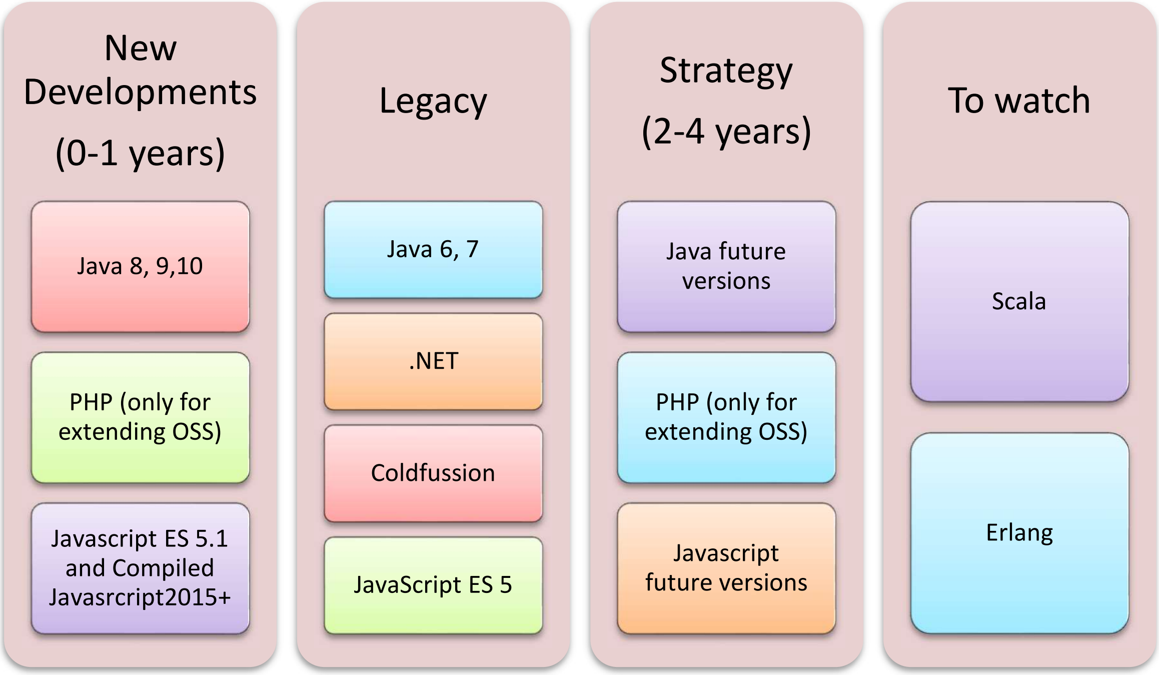
3.1 PROGRAMMING LANGUAGES

We will distinguish between development and scripting languages. While development languages are used to implement the main business logic of the applications and normally are compiled or pre-compiled, scripting languages are usually interpreted and used for specific tasks where they are more efficient like dealing with files

3.1.1 Development Languages

Our main development language is Java; PHP is only used for customizing certain functionalities in PHP based Open Source Software packages as Drupal, Limesurvey, etc…

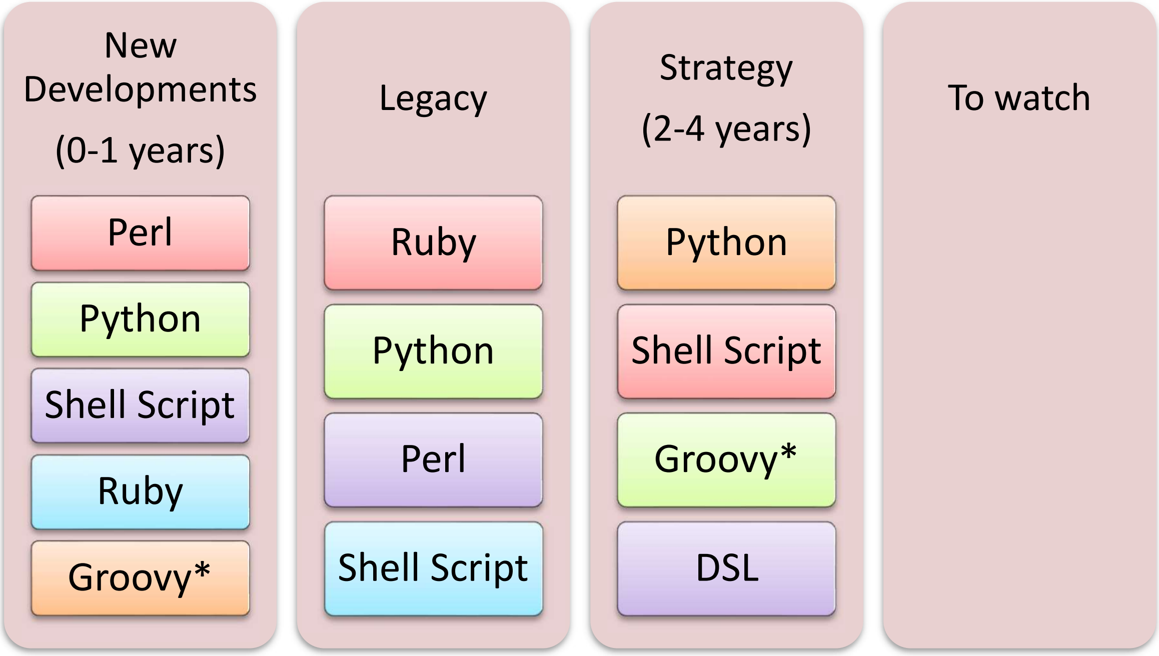
Web applications are based on the communication between the server side and the client side (browser). Javascript is the development language of the client side and it’s interpreted by the browser but it can be precompiled and can implement business logic. According to this and the standardization based on ECMA and the push of good practices within the Javascript community it has been included in this section.



New Developments (0-1 years)	Legacy	Strategy (2-4 years)	To watch
Java 8, 9,10	Java 6, 7	Java future versions	Scala
PHP (only for extending OSS)	.NET	PHP (only for extending OSS)	Erlang
Javascript ES 5.1 and Compiled Javasrcript2015+	Coldfussion	Javascript future versions	
	JavaScript ES 5		

3.1.2 Scripting Languages

Neither of the languages in this chapter should be used without an exception granted by Architecture as main programming language for new applications.



New Developments (0-1 years)	Legacy	Strategy (2-4 years)	To watch
Perl	Ruby	Python	
Python	Python	Shell Script	
Shell Script	Perl	Groovy*	
Ruby	Shell Script	DSL	
Groovy*			

*Groovy will be used as scripting and support language for configuring and extending functionalities in certain products like soapUI, ESB and BPM.

3.2 APPLICATION SERVERS

We will divide them between Java application Servers and Webservers.

Java Application Servers are tools that provide services for executing Java applications. These services are compatible with a set of standards released as Java Enterprise Edition (JEE) specification.

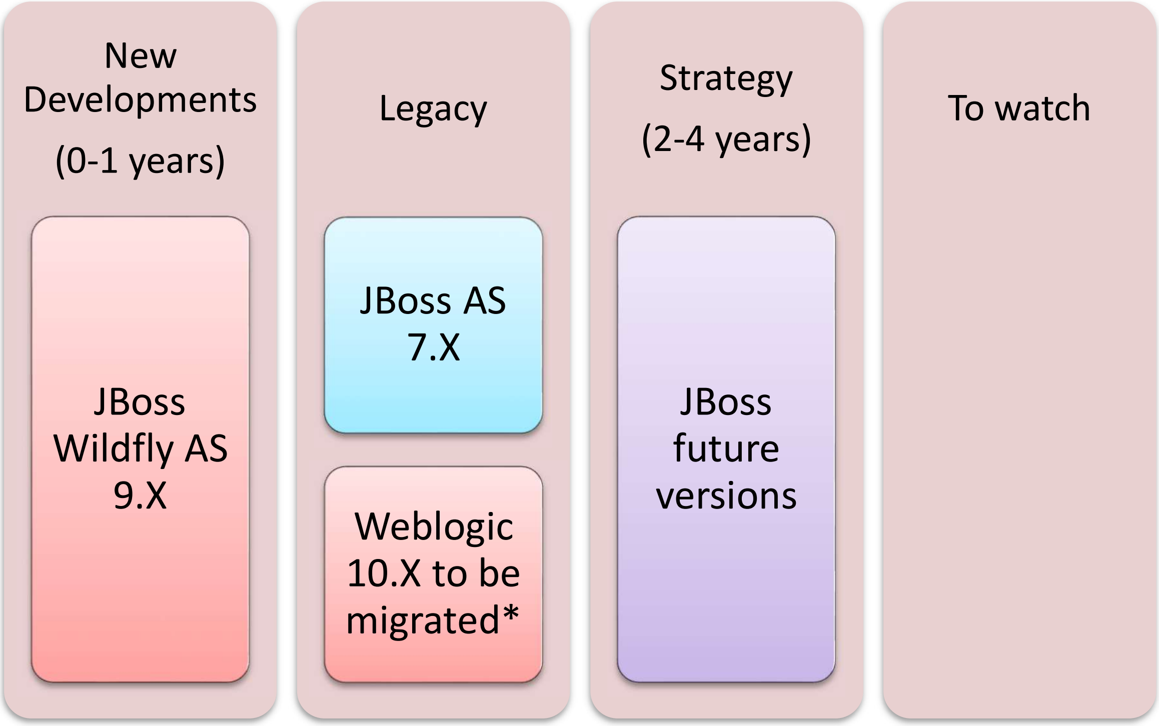
Web Servers are tools that help to serve web content through the Internet.

3.2.1 Java Application Servers

In this section we will consider not only Java Enterprise Edition Full Profile Application Servers which are the ones that support the full set of standards in the Java Enterprise Edition specification but also the Application Servers that supports the standards in the Web Profile specification.

After the big success of the adoption of JBoss at EUIPO and National Offices participating in Cooperation Fund programme, the strategy for Application Servers is to consolidate everything under JBoss. Previous versions of JBoss must be migrated into JBoss Wildfly (9.X version). This is compatible with EUIPO strategy of using Open Source software.

For new developments, especially those based on microservices, is not recommended the usage of application servers and the long term strategy of the office is moving to a “containerless” architecture. Only on those scenarios where is really required (e.g. JCA connectors) or when working with legacy applications we should consider the usage of a JEE Application server.



New Developments (0-1 years)

JBoss Wildfly AS 9.X

Legacy

JBoss AS 7.X

Weblogic 10.X to be migrated*

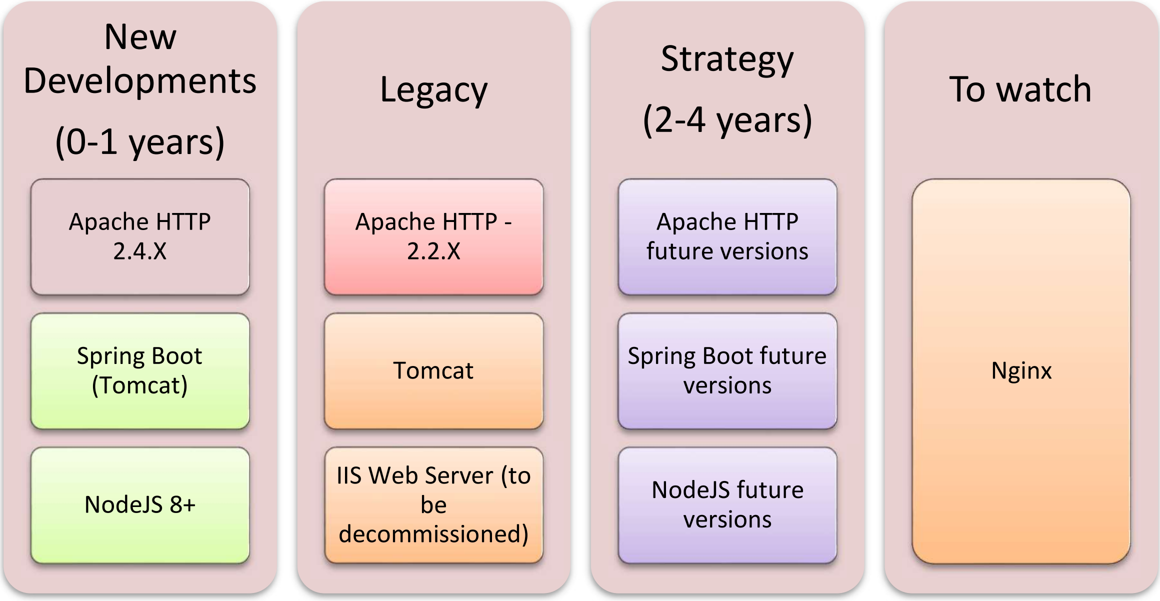
Strategy (2-4 years)

JBoss future versions

To watch

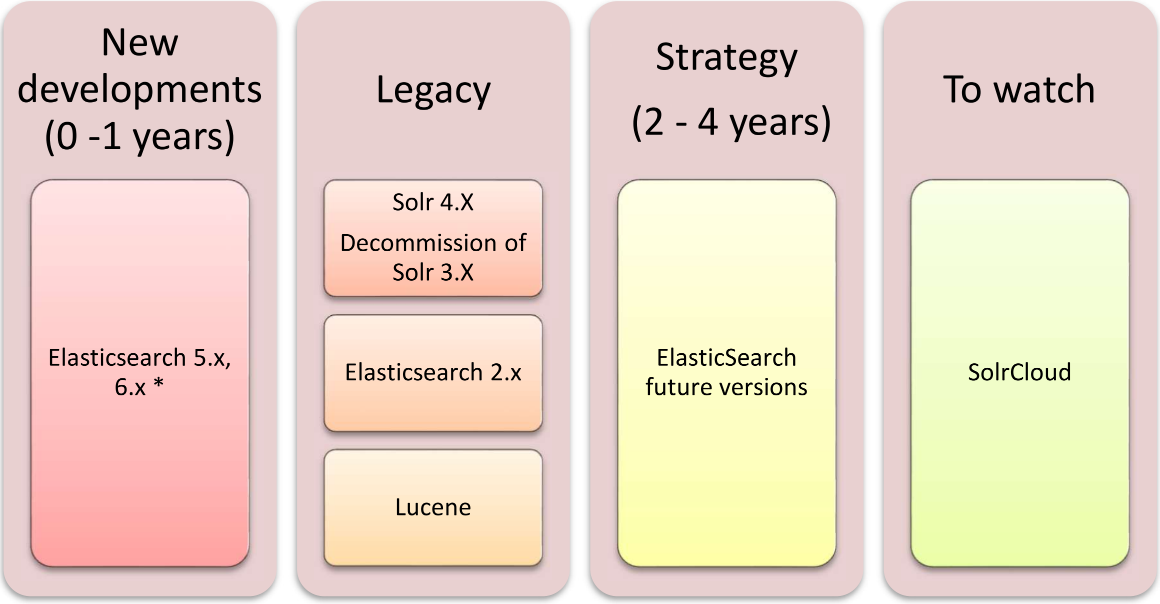
*Weblogic can be used for extending systems already using Weblogic.

3.2.2 Webservers



New Developments (0-1 years)	Legacy	Strategy (2-4 years)	To watch
Apache HTTP 2.4.X	Apache HTTP - 2.2.X	Apache HTTP future versions	Nginx
Spring Boot (Tomcat)	Tomcat	Spring Boot future versions	
NodeJS 8+	IIS Web Server (to be decommissioned)	NodeJS future versions	

3.3 SEARCH FRAMEWORKS

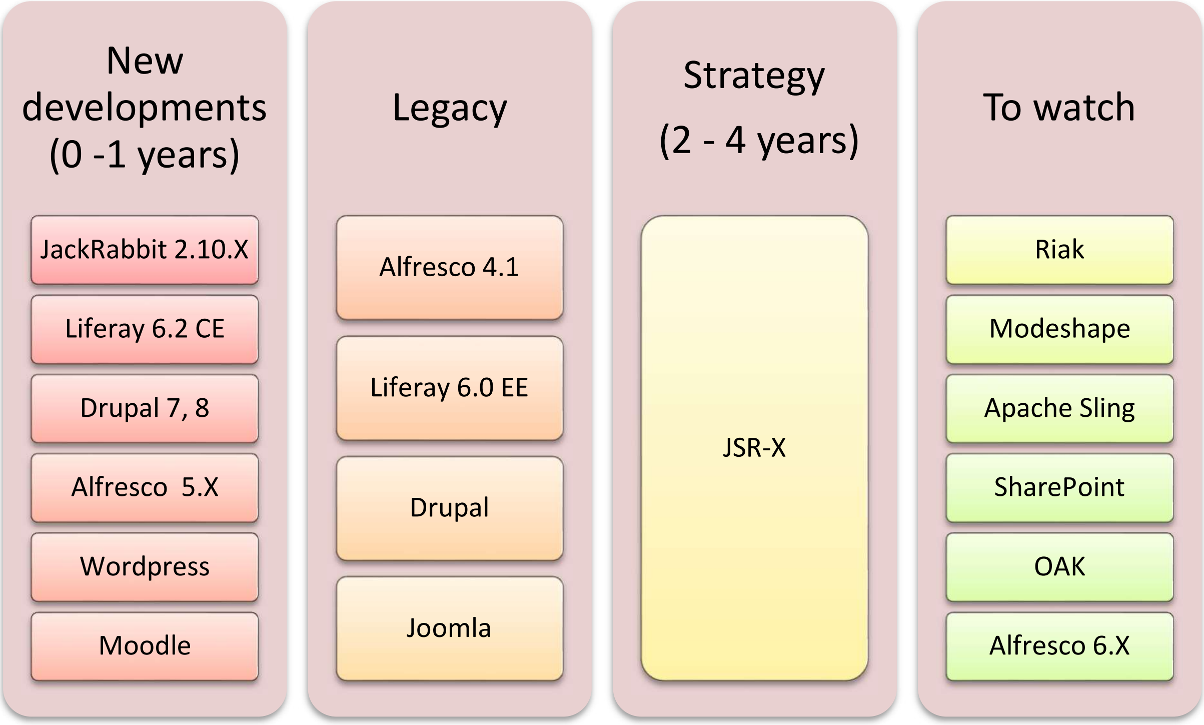


New developments (0 -1 years)	Legacy	Strategy (2 - 4 years)	To watch
Elasticsearch 5.x, 6.x *	Solr 4.X Decommission of Solr 3.X	ElasticSearch future versions	SolrCloud
	Elasticsearch 2.x		
	Lucene		

*Due to the frequent release cycle of these tools, and the fact that EUIPO does not need to be an early adopter, but a mainstream one, the version to be installed in production is according to the rule new development can use a version which is 3 months old.

3.4 DOCUMENT, WEB AND CONTENT MANAGEMENT PLATFORMS

The default Web Content Management for heavy sites should be Liferay and for medium-small size Drupal is the better choice.



New developments (0 -1 years)

JackRabbit 2.10.X
Liferay 6.2 CE
Drupal 7, 8
Alfresco 5.X
Wordpress
Moodle

Legacy

Alfresco 4.1
Liferay 6.0 EE
Drupal
Joomla

Strategy (2 - 4 years)

JSR-X

To watch

Riak
Modeshape
Apache Sling
SharePoint
OAK
Alfresco 6.X

3.5 HIGH AVAILABILITY

3.5.1 Service Provisioning

When defining new IT services, the pre-production and production environments should be provisioned following a 2N site cluster configuration. This means that our systems will be deployed in HA not only in one site but in two and taking into account that the capacity will be provisioned at 100% on each site.

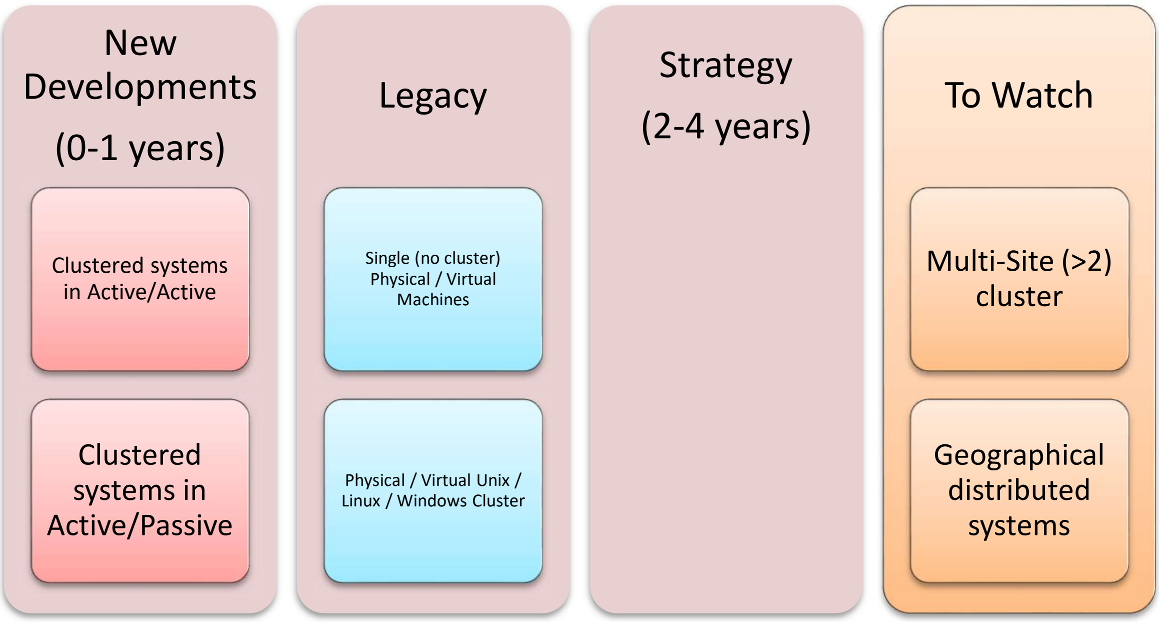
One (physical or virtual) leg of the cluster will reside within the Data Centre in Agua Amarga (AE42 DC) and the other leg within the other site at BUC (Backup Data Centre) in B. Sabadell premises. As far as possible, service will be provisioned in active-active mode as if we only had one (extended) data centre.

In case an active-active service could not be deployed, then high availability will be provided through:

- Replication accomplished at the application layer first, then on a database basis in second term, and lastly on an operating system basis (through LVM at the volume layer or with hypervisor capabilities if applicable).
- If none of the choices above are available because of extended requirements, then we shall use the storage array based (synchronous mode preferred versus asynchronous) or the network based replication.

Service integrity will be provided by configuring consistency groups when replicating at the storage block level. Any other type of replication will be evaluated prior to its implementation so every involved applications or systems can be set.

For specific critical services, a cloud provider may be used.


New Developments
(0-1 years)
Clustered systems in Active/Active
Clustered systems in Active/Passive
Legacy
Single (no cluster) Physical / Virtual Machines
Physical / Virtual Unix / Linux / Windows Cluster
Strategy
(2-4 years)
To Watch
Multi-Site (>2) cluster
Geographical distributed systems

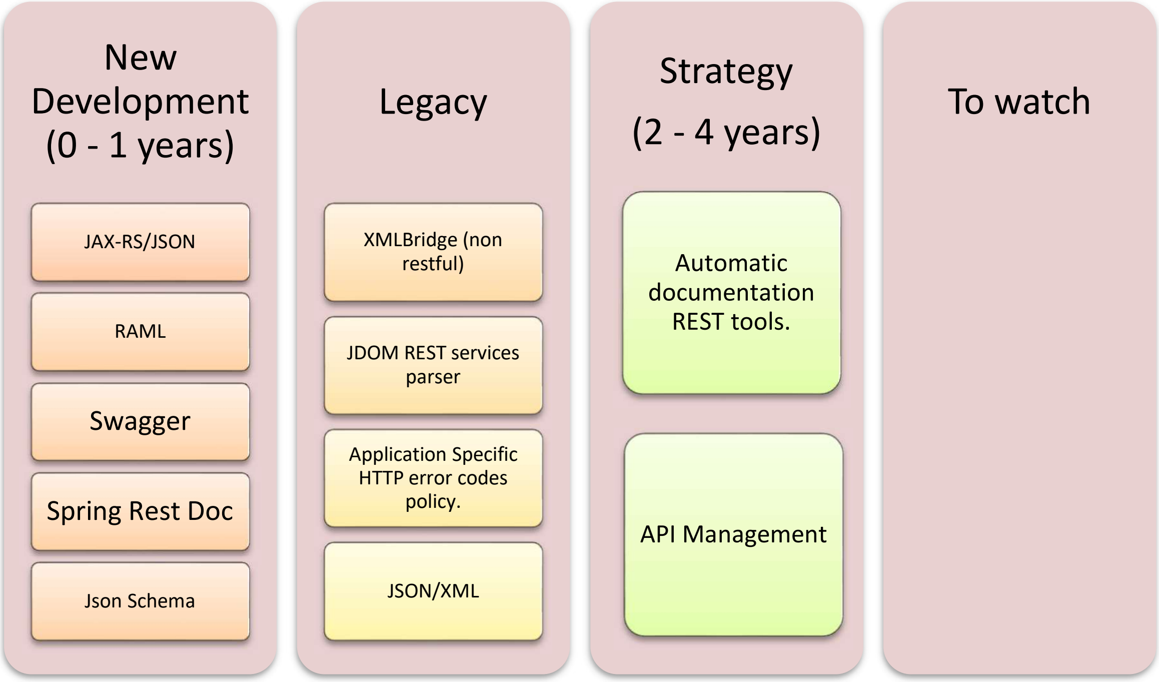
3.5.2 Backup Data Centre

Our backup data centre is located at the Banco Sabadell premises. The data centre interconnections (DCI) for Ethernet and fiber allow the deployment of active-active solutions. When this is not possible due to ‘legacy’ technology, proper restore and recover procedures should be tested and documented prior to go live.

4 Application Services

REST will be used to define any functional requirement that needs to be exposed as a service. Old legacy applications will be moved to a loosely coupled SOA approach, where services are the central unit for the integrations among systems.

4.1 REST


New Development (0 - 1 years)
JAX-RS/JSON
RAML
Swagger
Spring Rest Doc
Json Schema
Legacy
XMLBridge (non restful)
JDOM REST services parser
Application Specific HTTP error codes policy.
JSON/XML
Strategy (2 - 4 years)
Automatic documentation REST tools.
API Management
To watch

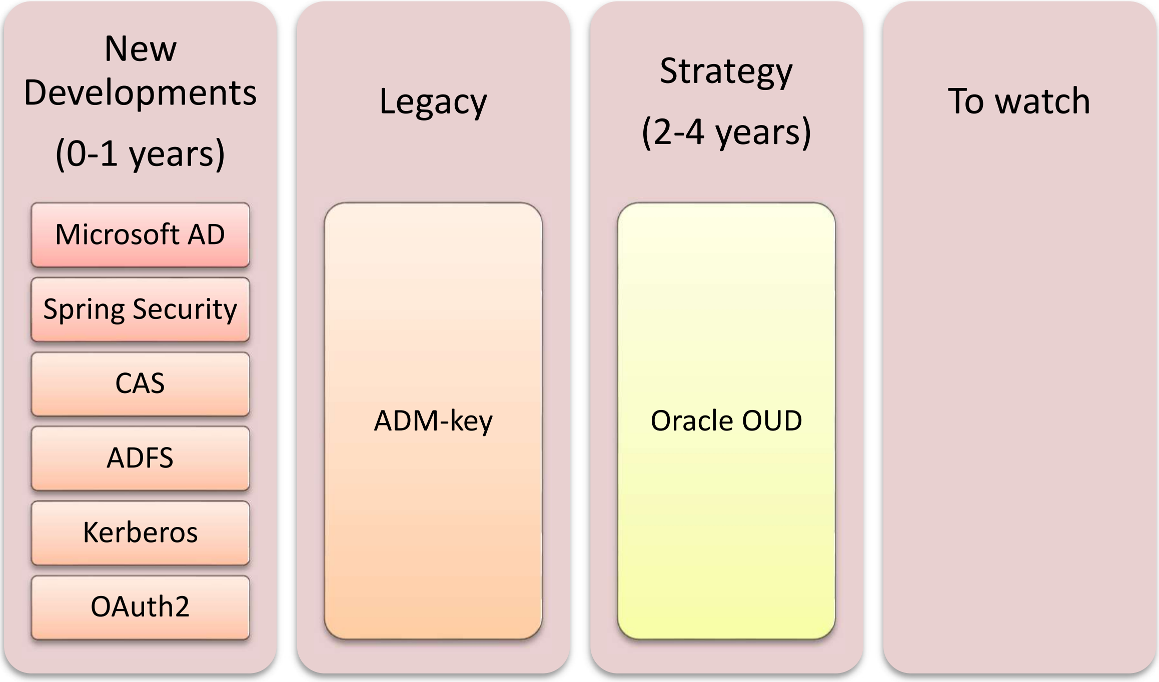
4.2 SECURITY

All services implemented in the office containing sensible data should cypher the message content, hiding the information and preventing sniffing attacks. In addition, all functionality exposed can only be provided to authenticated and authorized users.

Current ADM-Key will not be used for new development. For REST services OAuth2 is the authentication/authorization standard to be used. Spring Security will be the framework to support authentication.

For content encryption, WS-Security will be used for SOAP services while REST services will rely on transport encryption by using https.

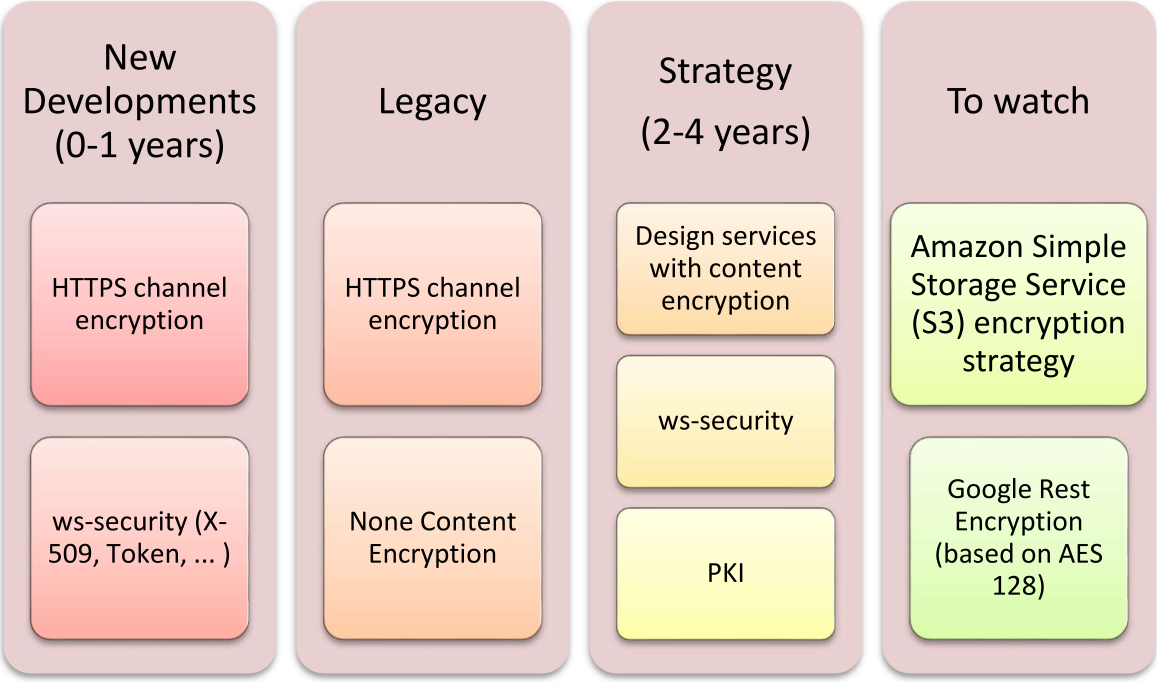
4.2.1 Authorization and Authentication



New Developments (0-1 years)	Legacy	Strategy (2-4 years)	To watch
Microsoft AD Spring Security CAS ADFS Kerberos OAuth2	ADM-key	Oracle OUD	

Exception: ADM-key can be used for new core business applications when they have to integrate with legacy systems. This has to be accepted by IT architecture team.

4.2.2 Encryption



New Developments (0-1 years)	Legacy	Strategy (2-4 years)	To watch
HTTPS channel encryption	HTTPS channel encryption	Design services with content encryption	Amazon Simple Storage Service (S3) encryption strategy
ws-security (X-509, Token, ...)	None Content Encryption	ws-security	Google Rest Encryption (based on AES 128)
		PKI	

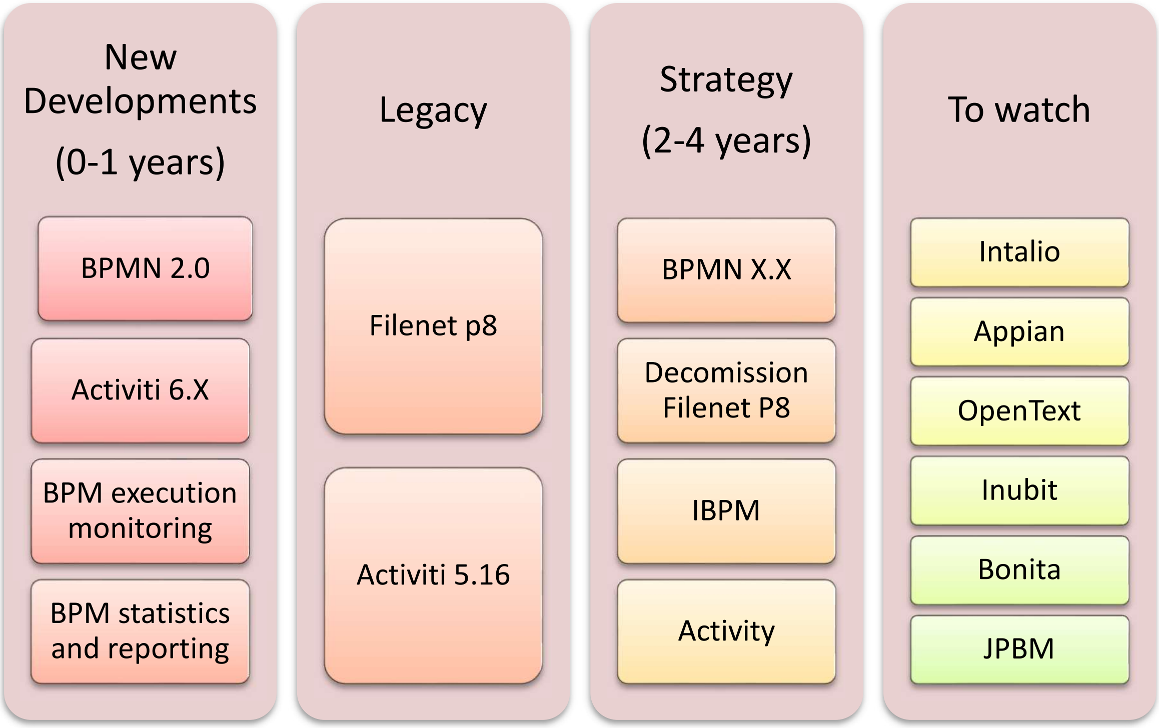
5 Processes/Workflows

Rules engine will contain the list of business rules that can be applied in the different BPM processes; it also includes a rules repository where the rules are registered. USE DSL when the rules need to be read and validated by domain experts (such as business analysts, for instance) who are not programmers; it hides implementation details and focuses on the rule logic proper.

5.1 PROCESS/WORKFLOWS ENGINES

New processes should be defined using a BPMN 2.0 notation. Business analysts will define a high level process definition, helped by a senior BPMN developer/designer. That high level model will be enhanced with technical details, producing a first process to be simulated. A tool for simulating the BPM process before its deployment could be used to test the different business scenarios.

Finally, the new developments should support reporting and monitoring of the process execution. This will be provided by the BPM Suite (BPMS). Currently the office has been working with Activiti 5.16.X but future developments will go with the latest version (Activiti 6).



New Developments (0-1 years)

BPMN 2.0

Activiti 6.X

BPM execution monitoring

BPM statistics and reporting

Legacy

Filenet p8

Activiti 5.16

Strategy (2-4 years)

BPMN X.X

Decomission Filenet P8

IBPM

Activity

To watch

Intalio

Appian

OpenText

Inubit

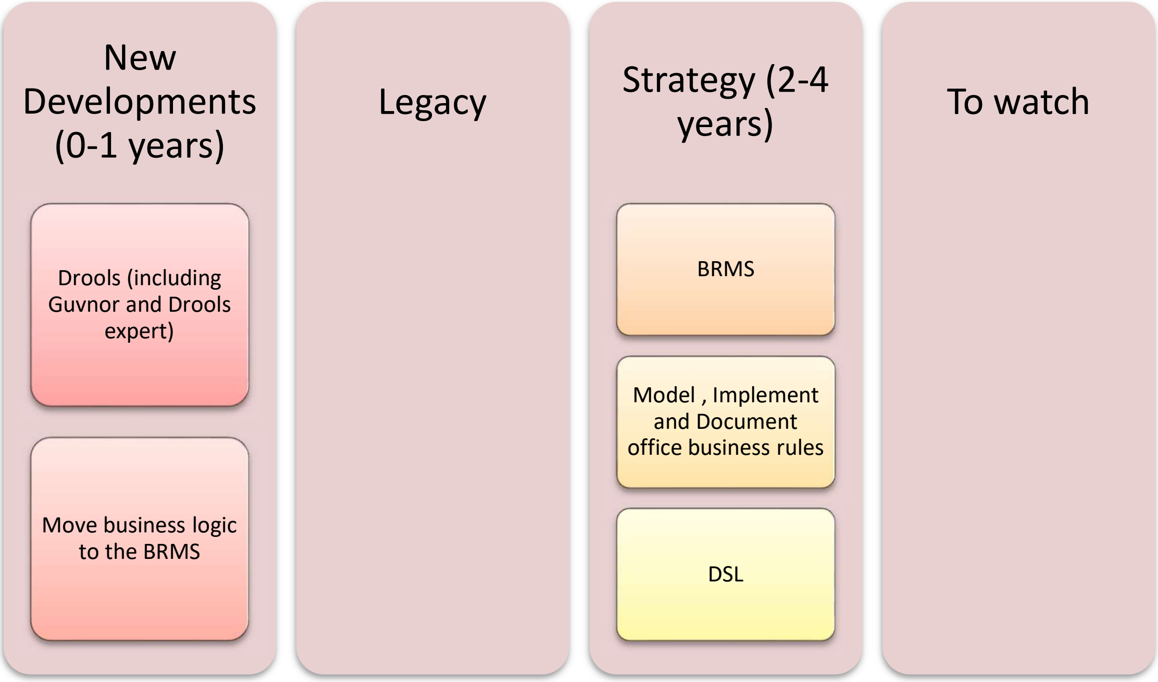
Bonita

JPBM

5.2 RULES & BUSINESS RULES MANAGEMENT SYSTEM (BRMS)

All new developments should use a BRMS to define all business rules and integrate them with the process flow engine and the new code. The BRMS will also include a rules repository where the business rule could be queried. New development could be based on Drools that incorporates a governance package (GUVNOR) and a coding environment (Drools expert).

The usage of a Domain Specific Language (DSL) is desired in order to hide technical complexity to the business and to allow template definitions.



New Developments (0-1 years)

Drools (including Guvnor and Drools expert)

Move business logic to the BRMS

Legacy

Strategy (2-4 years)

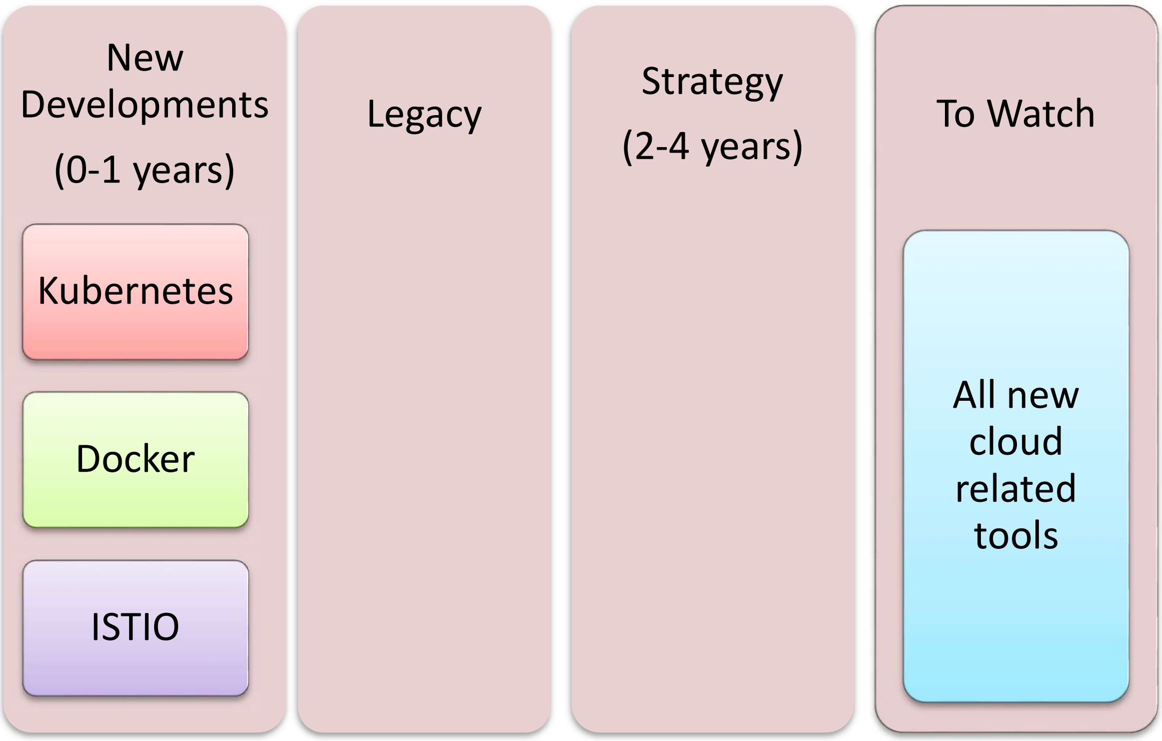
BRMS

Model , Implement and Document office business rules

DSL

To watch

6 Containers and Container Orchestration



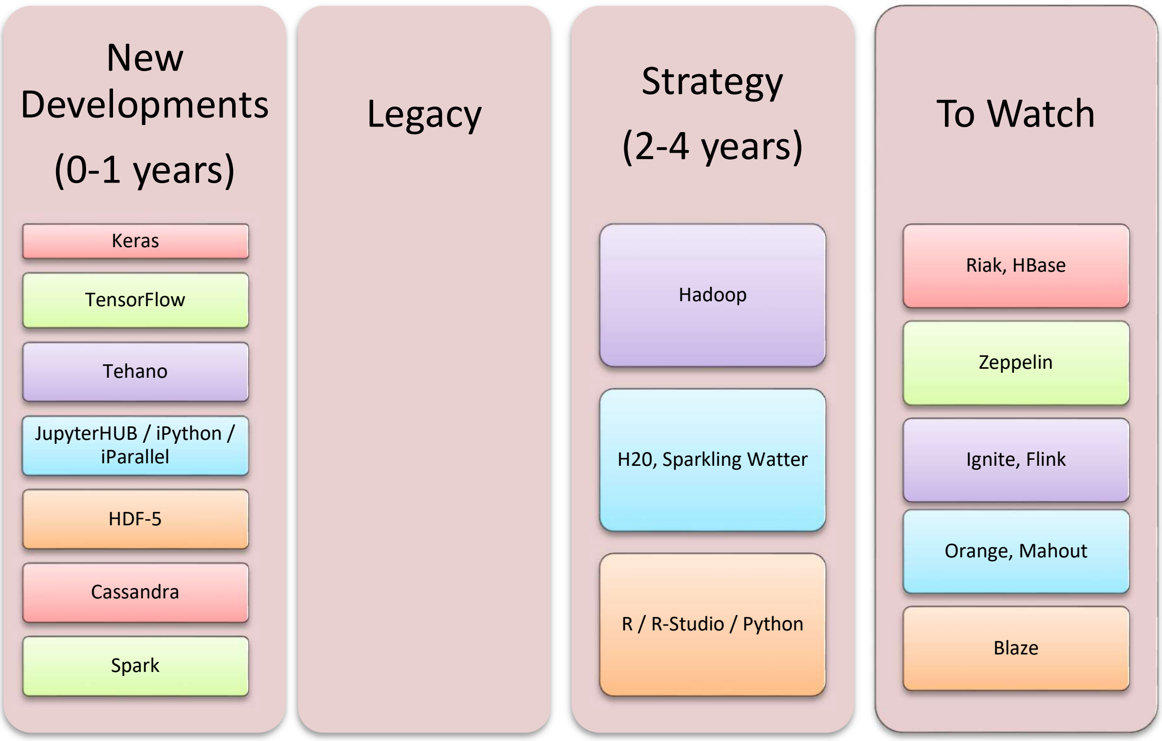
New Developments (0-1 years)	Legacy	Strategy (2-4 years)	To Watch
Kubernetes Docker ISTIO			All new cloud related tools

7 Big Data and Machine Learning

This chapter has evolved from Non-SQL databases to Big Data in order to consider other technologies.

This type of technologies shall be used only for supporting middleware products and not as a repository for developing new applications.

Ideally wrappers and plugins can be installed in order to query and model data using SQL-like grammar.



New Developments (0-1 years)

- Keras
- TensorFlow
- Tehano
- JupyterHUB / iPython / iParallel
- HDF-5
- Cassandra
- Spark

Legacy

Strategy (2-4 years)

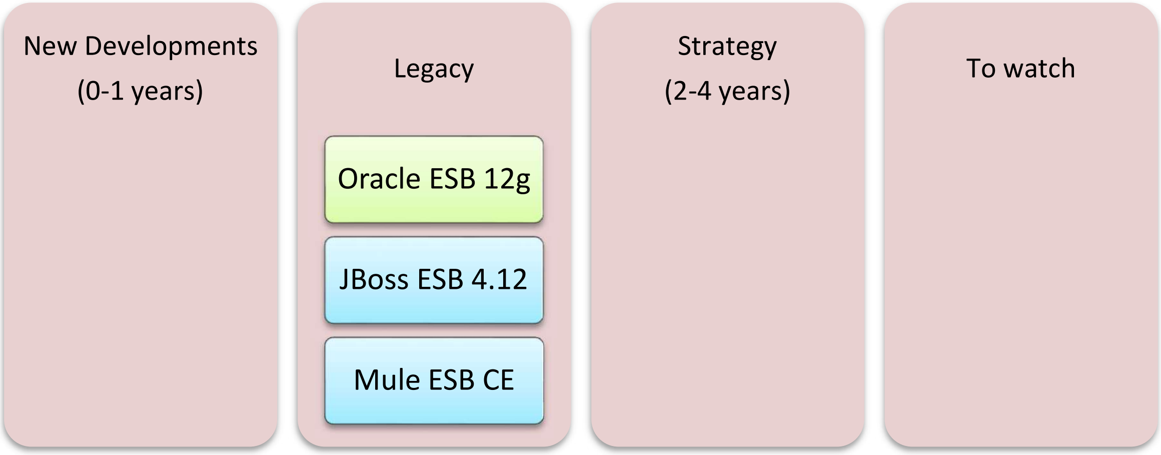
- Hadoop
- H20, Sparkling Watter
- R / R-Studio / Python

To Watch

- Riak, HBase
- Zeppelin
- Ignite, Flink
- Orange, Mahout
- Blaze

8 Middleware

8.2 ESB

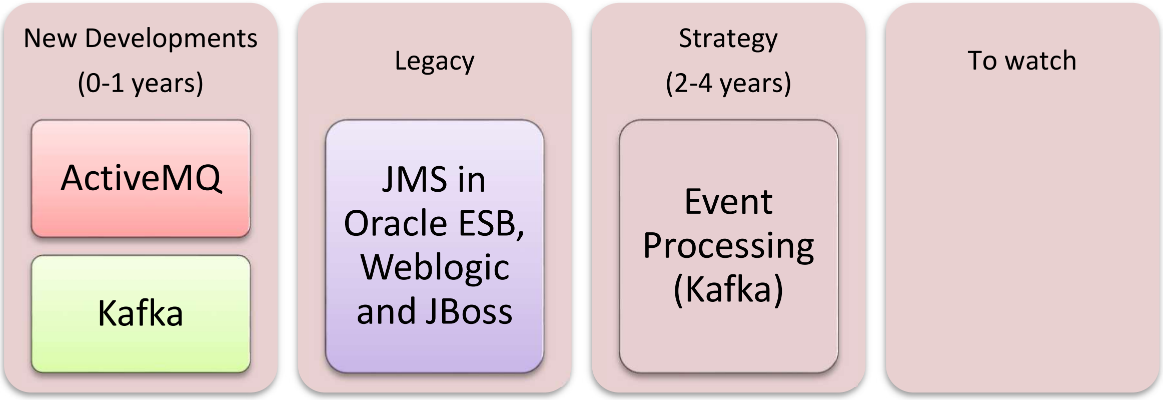


New Developments (0-1 years)	Legacy	Strategy (2-4 years)	To watch
	Oracle ESB 12g JBoss ESB 4.12 Mule ESB CE		

8.3 MESSAGING

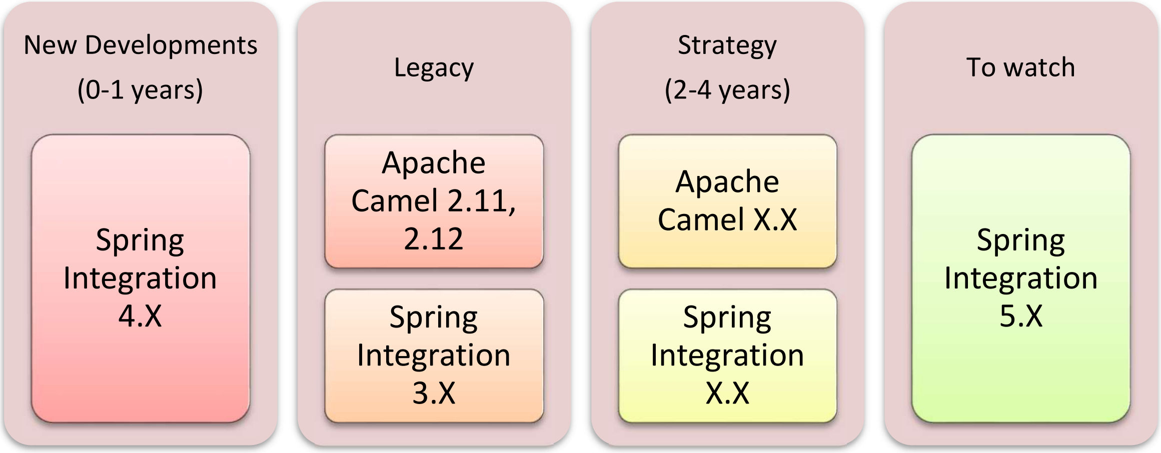
For future developments KAFKA is the desired messaging system to be used as it provides a high throughput, easy management, move the complexity from the server to the consumers. Nevertheless, we will continue using traditional JMS, with the latest ActiveMQ version for existing systems where adding a dependency with Kafka could be too complex or unfeasible.

According to this new strategy:



New Developments (0-1 years)	Legacy	Strategy (2-4 years)	To watch
ActiveMQ Kafka	JMS in Oracle ESB, Weblogic and JBoss	Event Processing (Kafka)	

8.4 INTEGRATION FRAMEWORKS



New Developments (0-1 years)	Legacy	Strategy (2-4 years)	To watch
Spring Integration 4.X	Apache Camel 2.11, 2.12	Apache Camel X.X	Spring Integration 5.X
	Spring Integration 3.X	Spring Integration X.X	

8.5 LOAD BALANCING

For load balancing, the architecture foresees 2 possibilities:

1. Hardware solution: Big-IP F5 Load Balancer shall be used to provide intelligent Load Balancing capabilities, and to provide policy-based web application security against the top OWASP threats. This hardware solution has to be used for the applications that are exposed to Internet.
2. Software solution: HA Proxy: an open source load balancer that has to be used for applications not accessible from Internet or applications with less traffic.

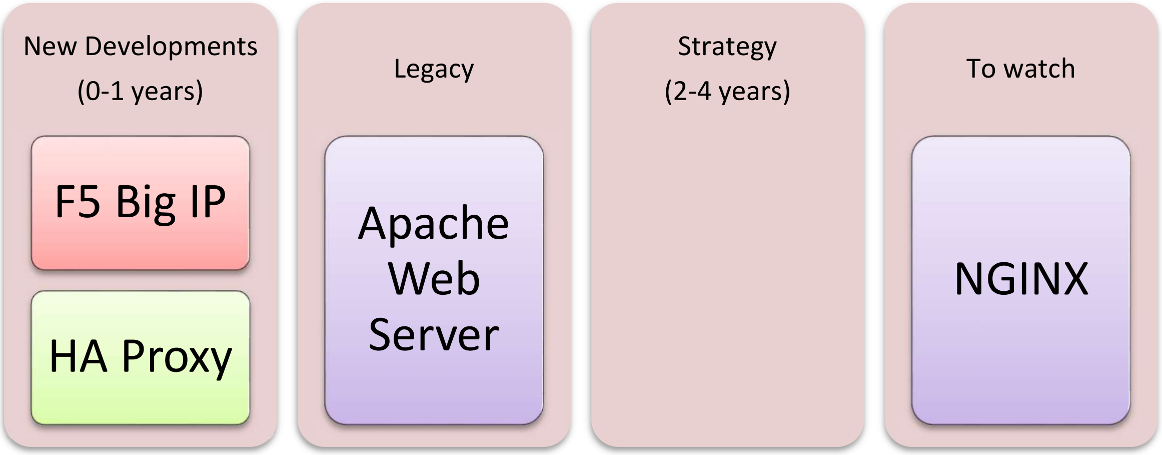
The IT Architect has to choose between these 2 alternatives, and some other criteria could impact the final solution, e.g.

- The importance of the traffic of an internal application making the choice of F5 safer
- The need of an open source solution, an argument in favor of HA Proxy
- The criticality of the traffic to be balanced: e.g. LDAP traffic is balanced by F5 due to the fact that this service is critical for the whole office.
- Infrastructure services should be balanced by F5 to prevent any system dependencies.

HA proxy has to be used as an infrastructure service: a pool of server by environment / group of applications. It has to be installed using the installation scripts.

Big-IP F5 shall not be used as middleware for integrating applications, as this is not its purpose. It shall not be used as the unique security mechanism of web and internal applications. Applications shall implement the needed protection measures in order to avoid programmatically the threads described in the IT Standards. F5 Application Security Module (Web Application Firewall functionality) will provide an extra security layer to the external services. F5 shall not apply WAF rules to calls between internal applications.

Static Content can be cached at F5.



New Developments (0-1 years)

F5 Big IP

HA Proxy

Legacy

Apache Web Server

Strategy (2-4 years)

To watch

NGINX

9 Databases

A distinction between In-house and Third party applications/products has to be applied at the time of indicating which databases are accepted.

9.1 IN-HOUSE APPLICATIONS

For in-house applications apply a distinction between relational and NO-SQL databases.

Our In-house applications shall follow a relational DB model. NO-SQL databases shall not be used at the moment. A PoC shall be launched in the near future with some of these DBs in order to select the most interesting for us.

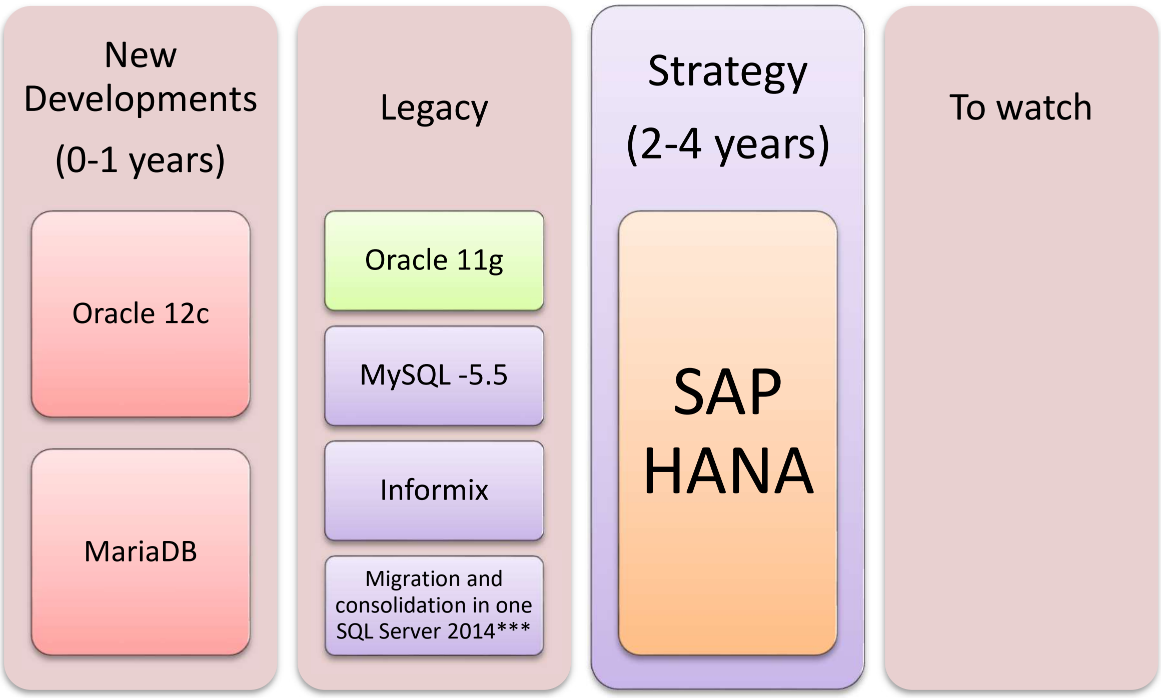
9.1.1 Relational Databases

Related to Relational DB, we adopt Oracle as the main DB for in-house and COTS application.

Any critical system shall use Oracle as DB, as our Oracle installation provides High Availability at DB level. (Oracle RAC).

MySQL shall be used only for OSS packages or for non-critical applications that will not require High Availability at DB level.

Client based DBs which are not enterprise server ready for multiusers like MS Access are not considered in this document. Using this type of DB engines will make sense only when data is non-critical and for support activities.



* MySQL should be transitioned into MariaDB.

**No new developments shall be done using Informix, but legacy systems need to be adapted if needed to work with Informix.

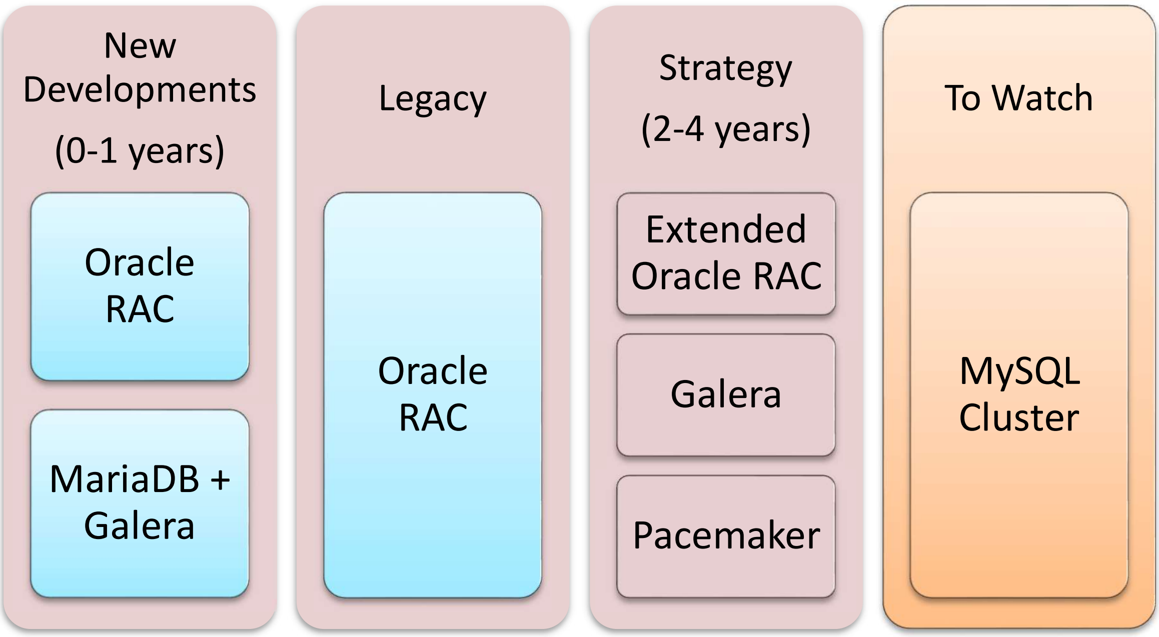
***Although no in-house development has been done at EUIPO using SQL Server as the main DB, certain COTS products used for the management of the infrastructure used SQL Server as default DB, for that reason a lot of different instances has been created. Tools that require an effective HA and Disaster Recovery approach shall be migrated into Oracle RAC/Data Guard architecture.

9.1.2 Relational DB High Availability

High Availability at DB level is guaranteed with Cluster solutions.

Oracle RAC will be used as Cluster solution for Oracle.

MySQL Cluster will NOT be used as only supports NDB, and the DB engine which is used at MySQL is InnoDB.



9.2 THIRD PARTY APPLICATIONS

As principle, if Oracle is supported by the Third Party application, this would be the preferred DB. If Oracle is not supported but MySQL is supported, then that would be the choice. In case, Oracle and MySQL will not be supported but is supported by other DB already deployed at EUIPO (e.g. SQL Server) then this could be accepted.

Informix shall not be used as an option as the strategy is decommissioning Informix in the future, and therefore the dependency of it shall be reduced.

9.3 HIGH AVAILABILITY

9.3.1 Service Provisioning

The Recovery Time Objective of each application is fixed by the Business Impact Analysis.

The services to be restored in 24 hours or less must be deployed in both EUIPO data centres in Active/Active mode – each data centre being able to independently provide 100% of the service.

In consequence, the Infrastructure Services that are providing service to applications to be restored in 24 hours or less have also to be deployed in Active/Active.

Data bases and shared file systems have to be replicated between both DCs, and running in Active/Active when the technology in place at the Office allows. In case an active-active service could not be deployed, then high availability will be provided through:

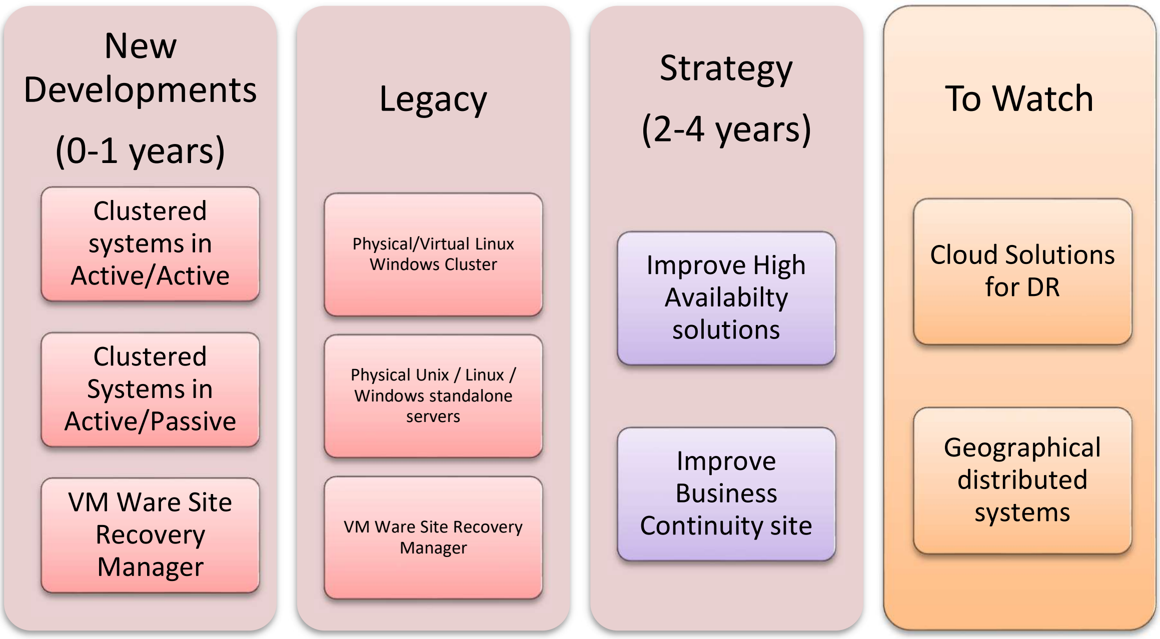
- Replication accomplished at the application layer first, then on a database basis in second term, and lastly on an operating system basis (through LVM at the volume layer or with hypervisor capabilities if applicable).
- If none of the choices above are available because of extended requirements, then we shall use the storage array based (synchronous mode preferred versus asynchronous) or the network based replication.

The services to be restored between 24 and 48 hours have to be deployed at least in Active/Standby (Hot or Warm), the active node(s) being located in the Agua Amarga data centre and the passive nodes in the backup centre.

The services to be restored in more than 48 hours shall be available at least in cold standby in the backup centre, e.g. using VM Ware Site Recovery Manager (version number has to be aligned with the VCenter version that is running in production environment).

For all applications, the data (databases and file systems) have to be synchronized between both data centres using at least disk replication mechanism, e.g. Hitachi True Copy.

Service integrity will be provided by configuring consistency groups when replicating at the storage block level. Any other type of replication will be evaluated prior to its implementation so every involved applications or systems can be set.


New Developments
(0-1 years)
Clustered systems in Active/Active
Clustered Systems in Active/Passive
VM Ware Site Recovery Manager
Legacy
Physical/Virtual Linux Windows Cluster
Physical Unix / Linux / Windows standalone servers
VM Ware Site Recovery Manager
Strategy
(2-4 years)
Improve High Availabilty solutions
Improve Business Continuity site
To Watch
Cloud Solutions for DR
Geographical distributed systems

9.4 BACKUP CENTRE AND BUSINESS CONTINUITY SITE

The second EUIPO data centre (DC) is now connected with quick and redundant telecommunication lines, with the result that both EUIPO DCs are now one logical DC (extended DC model).

The second DC is now called Backup Centre. It is not only ready to provide service in case of major disaster affecting the main DC but also when a single component fails, the corresponding backup component will provide the service. Refer to Service Provisioning chapter for the deployment rules to be applied in Backup Centre.

EUIPO also exploits a Business Continuity site located in London at the EMA. This DC has to provide business critical service (please refer to the Business Impact Analysis) in case of major disaster affecting EUIPO main DC and backup centre. As the resources in this DC are limited, a new application delivering such business critical service has to provide a standalone version, running without integration and allowing the import of the dossiers created during the disaster into the EUIPO full version once it will be available.

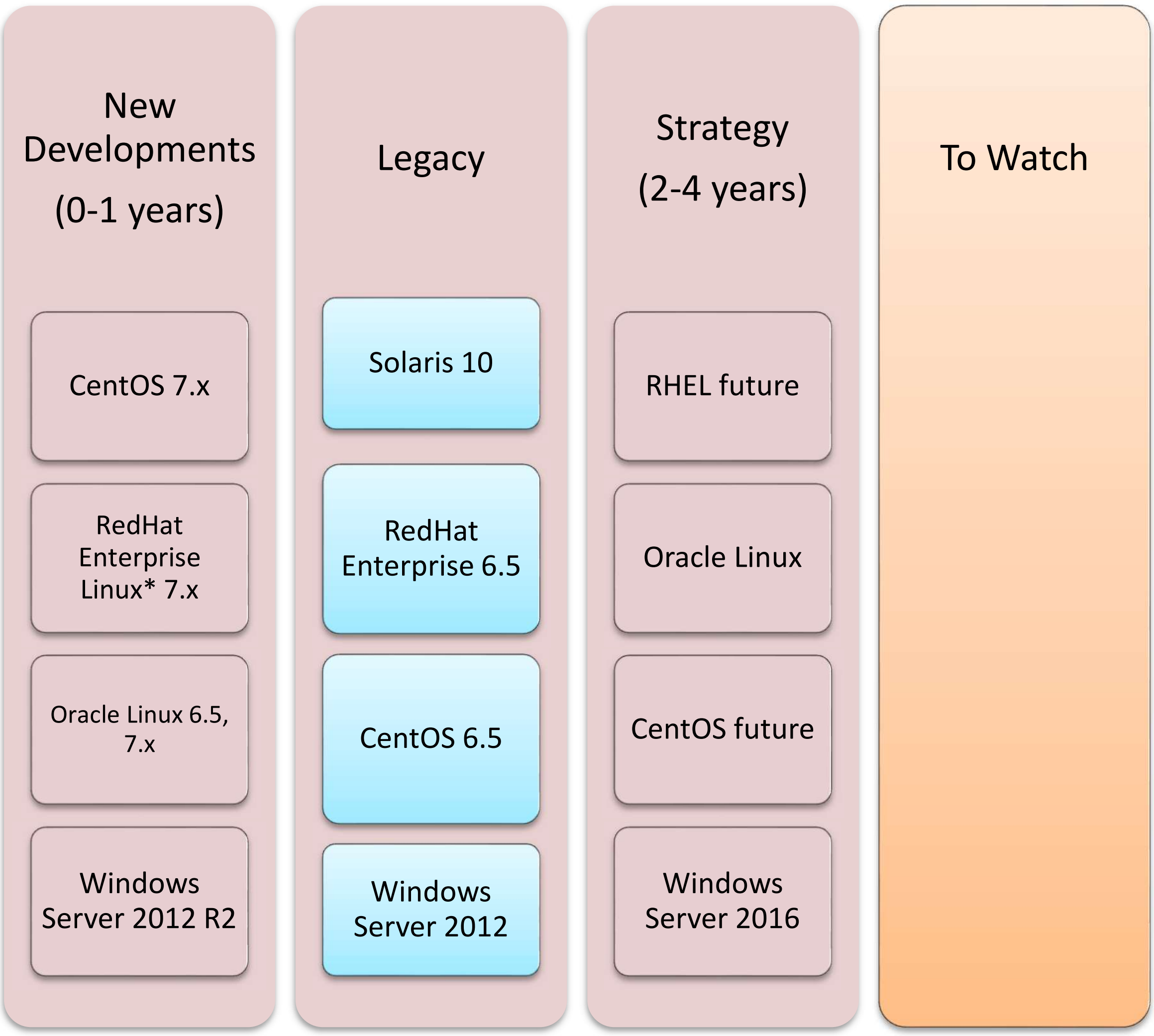
10 Operating Systems

10.1 CLIENT PLATFORMS

Please check 2.1.2

10.2 SERVER PLATFORMS

A big base exists in the current legacy. A big effort in consolidation of our platforms shall be made in order to simplify management, maintenance, budgeting and deployment.

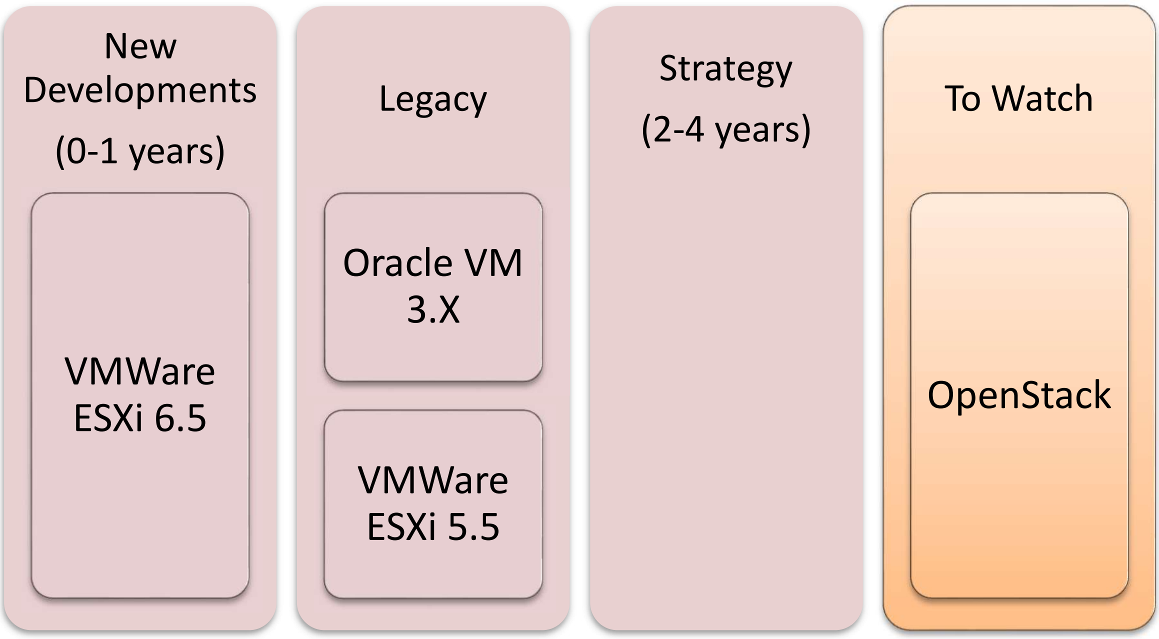


New Developments (0-1 years)	Legacy	Strategy (2-4 years)	To Watch
CentOS 7.x	Solaris 10	RHEL future	
RedHat Enterprise Linux* 7.x	RedHat Enterprise 6.5	Oracle Linux	
Oracle Linux 6.5, 7.x	CentOS 6.5	CentOS future	
Windows Server 2012 R2	Windows Server 2012	Windows Server 2016	

*RHEL will be used only for support reasons when Oracle Linux will not be a supported version.

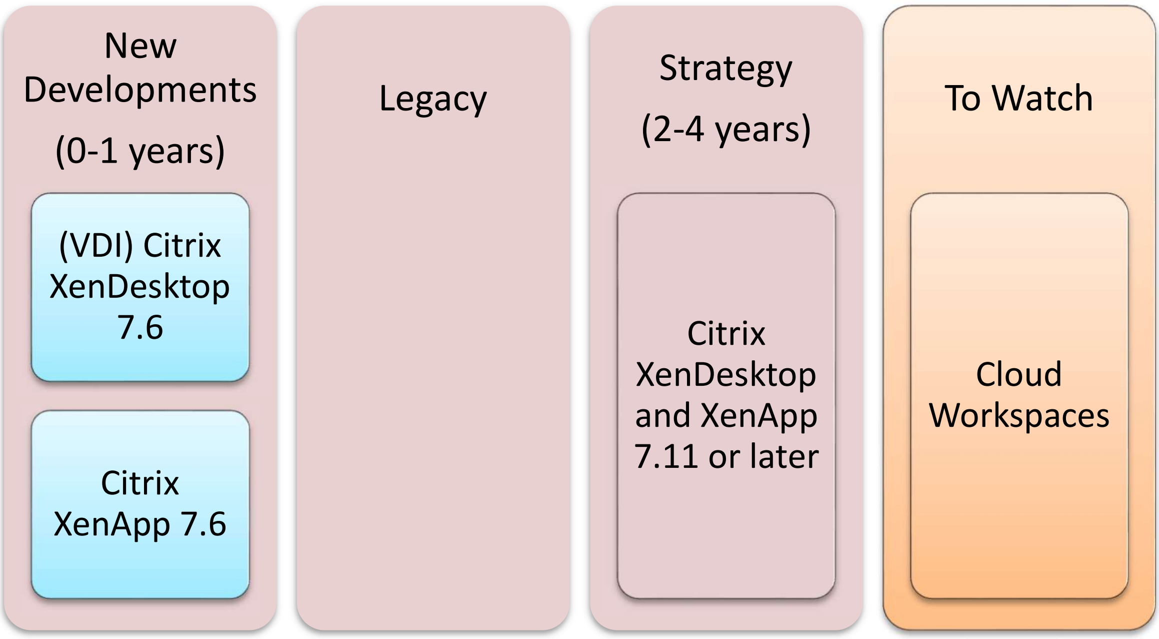
11 Virtualization

11.1 VIRTUAL SERVERS



New Developments (0-1 years)	Legacy	Strategy (2-4 years)	To Watch
VMWare ESXi 6.5	Oracle VM 3.X VMWare ESXi 5.5		OpenStack

11.2 VIRTUAL DESKTOPS



New Developments (0-1 years)	Legacy	Strategy (2-4 years)	To Watch
(VDI) Citrix XenDesktop 7.6 Citrix XenApp 7.6		Citrix XenDesktop and XenApp 7.11 or later	Cloud Workspaces

11.2.1 Private Cloud

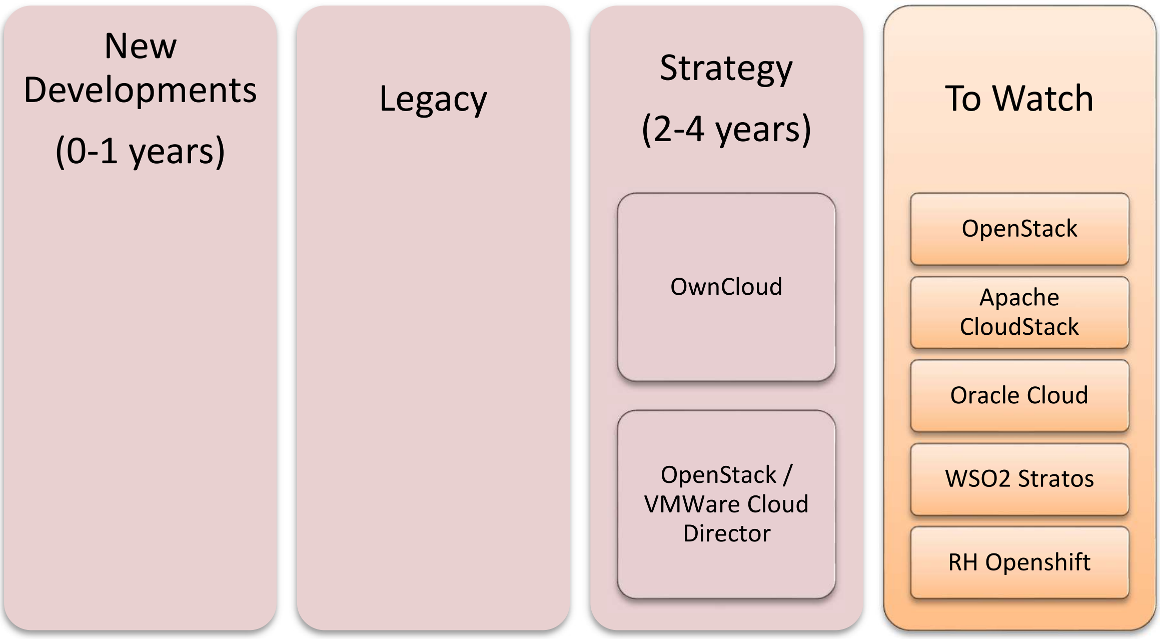
The virtualization of servers and adoption of a utility computing model is a tendency in the market. This implies the strategy of deploying at EUIPO the facilities to manage Private Clouds.

As part of the adoption and implementation of Private Clouds at EUIPO several solutions will be tested mainly focused in the areas of Object Storage, IaaS (Infrastructure as a Service) and PaaS (Platform as a Service).

An important area to consider will be to offer Storage based Infrastructure as a Service solution (OwnCloud) similar to the DropBox service. This will allow file sharing functionality through Internet but the data will reside at EUIPO premises instead that in external providers.

Another area to consider at the short term it is related to enhance our virtualization capability by the usage of IaaS cloud management solutions (OpenStack, CloudStack, VMWare Cloud Director, etc…)

Finally, solutions based on Platform as a Service should be watched at medium term, as offers the possibility of offering a powerful platform to host internal developed applications in an easy way.


New Developments (0-1 years)

Legacy

Strategy (2-4 years)

OwnCloud

OpenStack / VMWare Cloud Director

To Watch

OpenStack

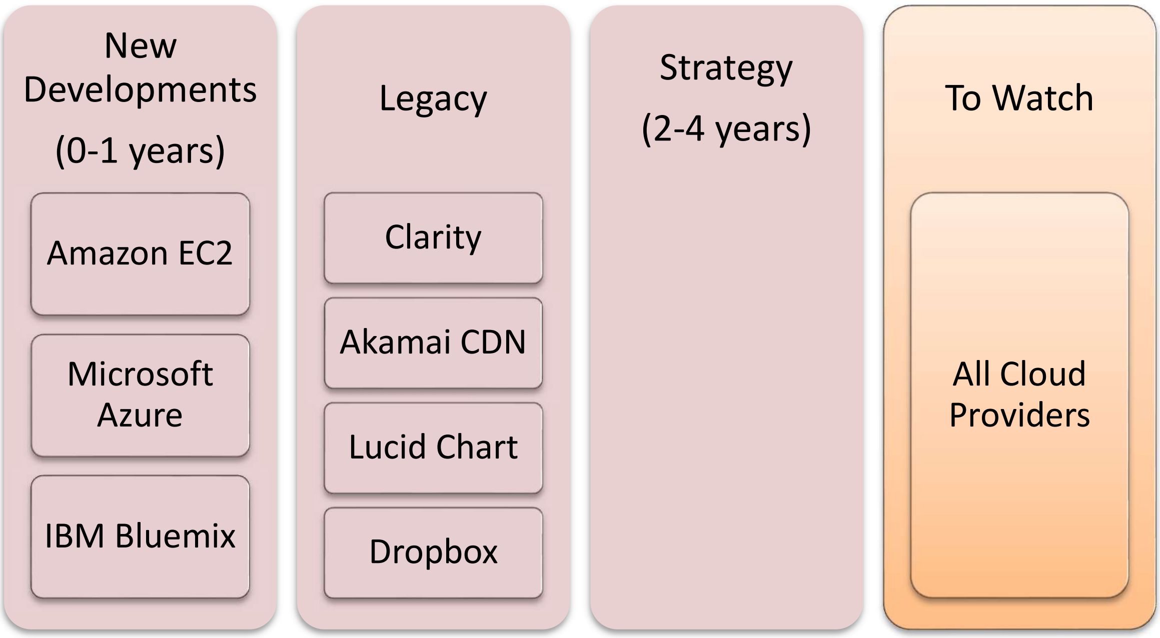
Apache CloudStack

Oracle Cloud

WSO2 Stratos

RH Openshift

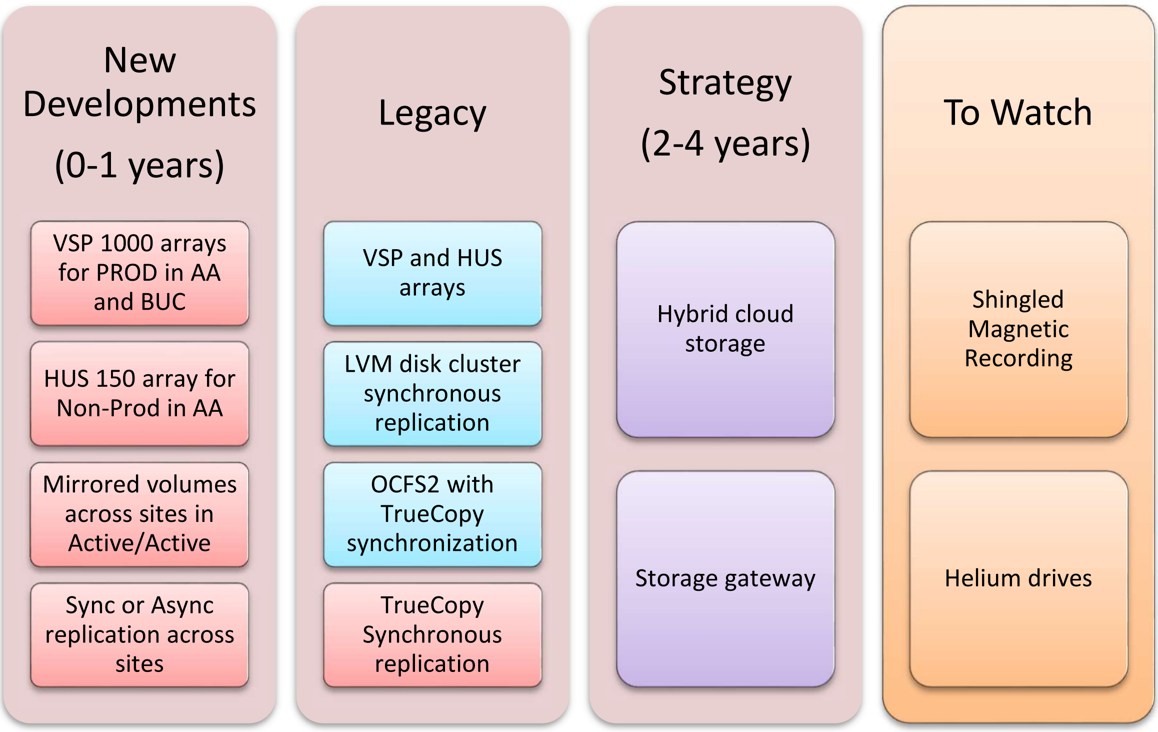
11.2.2 Public Cloud



New Developments (0-1 years)	Legacy	Strategy (2-4 years)	To Watch
Amazon EC2	Clarity		All Cloud Providers
Microsoft Azure	Akamai CDN		
IBM Bluemix	Lucid Chart		
	Dropbox		

12 Storage

12.1 STORAGE AREA NETWORK



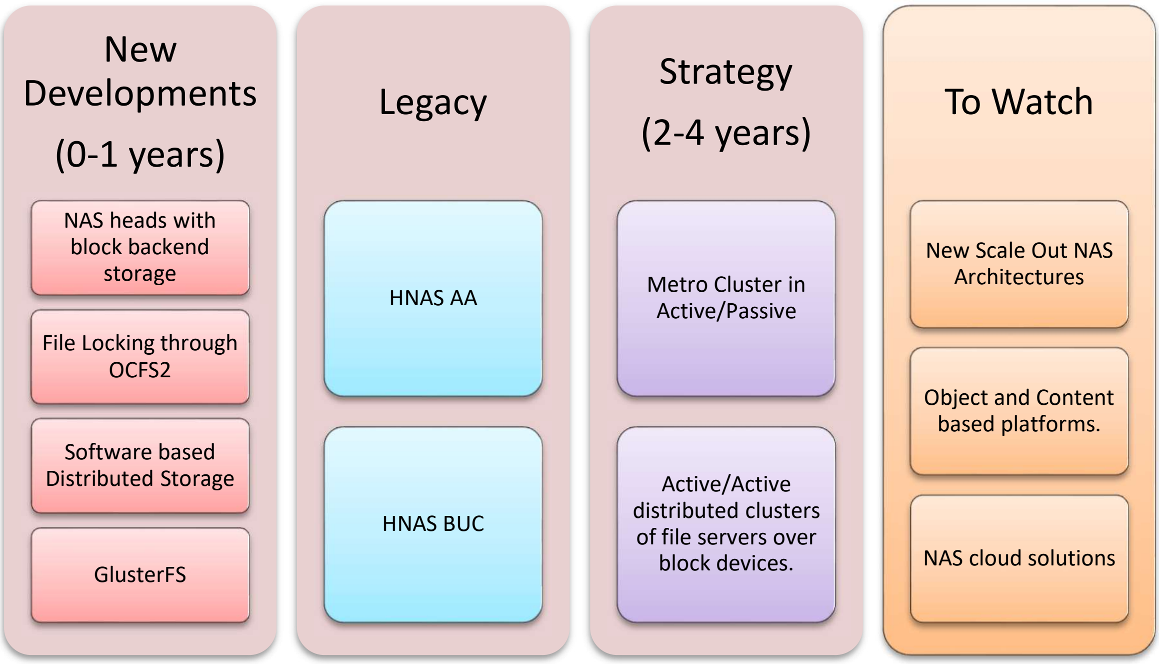
New Developments (0-1 years)	Legacy	Strategy (2-4 years)	To Watch
VSP 1000 arrays for PROD in AA and BUC	VSP and HUS arrays	Hybrid cloud storage	Shingled Magnetic Recording
HUS 150 array for Non-Prod in AA	LVM disk cluster synchronous replication	Storage gateway	Helium drives
Mirrored volumes across sites in Active/Active	OCFS2 with TrueCopy synchronization		
Sync or Async replication across sites	TrueCopy Synchronous replication		

This hybrid approach can allow an organisation to take advantage of the scalability and cost effectiveness of cloud storage without exposing mission-critical data. The challenge is to integrate and govern such a system, preferably without altering the existing on premise infrastructure or the applications. That is especially true when you consider services must be provisioned from different sources, yet must act and interact as a single system. This, in turn, means you need common data and software management tools.

Different suppliers try to solve this in different ways, including accessing everything via an Internet Small Computer System Interface (iSCSI), integrating primary storage with the cloud or via a cloud gateway of some sort, for example.

One of the most popular routes is a hybrid cloud storage appliance, which has intelligence, software and local storage built into it. Application servers communicate with the appliance and never directly to the cloud. By caching data locally, the appliance provides more bandwidth than the wide-area network, reduces bandwidth and storage costs, and minimises the effects of link latency. The appliance can also reduplicate and encrypt data before staging it in the cloud.

12.2 NETWORK ATTACHED STORAGE



New Developments (0-1 years)

- NAS heads with block backend storage
- File Locking through OCFS2
- Software based Distributed Storage
- GlusterFS

Legacy

- HNAS AA
- HNAS BUC

Strategy (2-4 years)

- Metro Cluster in Active/Passive
- Active/Active distributed clusters of file servers over block devices.

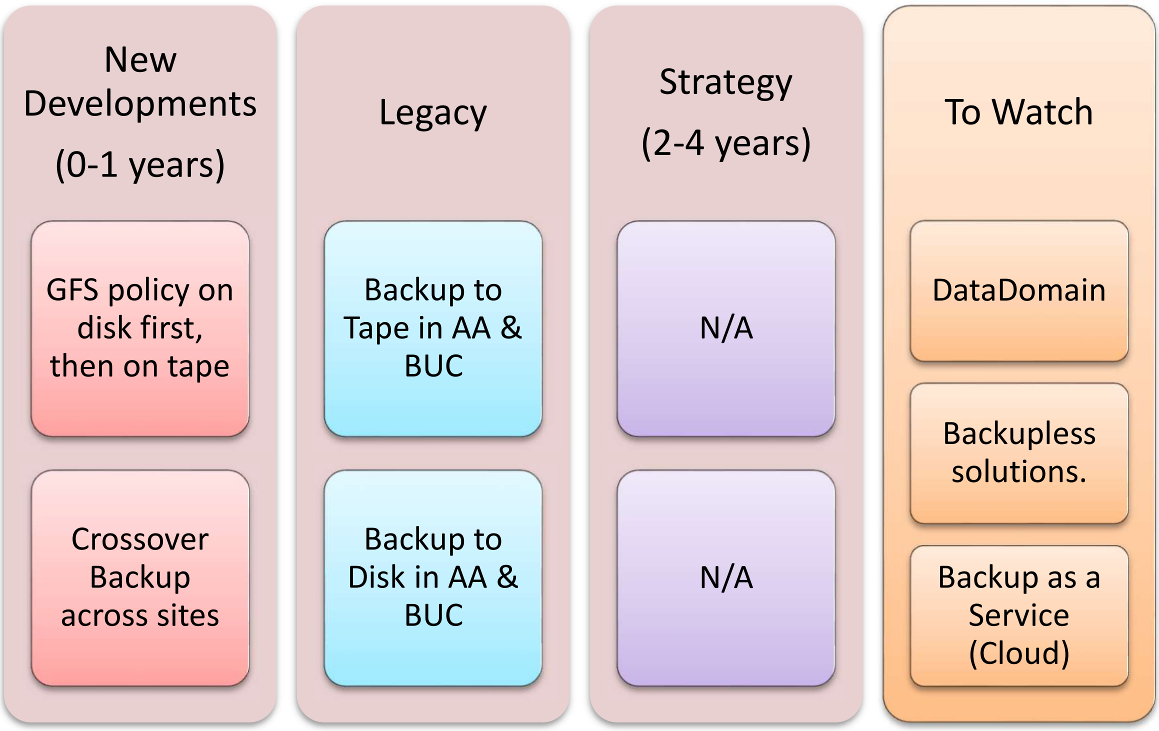
To Watch

- New Scale Out NAS Architectures
- Object and Content based platforms.
- NAS cloud solutions

Our current HNAS devices can currently provide filesystem services and can offer continuous block, file or content asynchronous replication across AA and BUC. But the RPO will not be zero and the RTOs are still complex and high. Proper procedures and a specific design for every IT file service hast to be defined previously as this area can evolve in a short term.

Therefore, the storage based on network protocols needs to be defined according to new architectures providing better capabilities regarding concurrency, performance, availability and recovery. Many of our systems providing millions of small files need innovative solutions based on active/active architectures or distributed file systems rather than in centralized ones. The development of some solutions based on open source can help to reach this goal. The evaluation and implementation of Software Defined Storage (SDS) solutions will let driving from the traditional scale-in to scale-out architectures.

12.3 BACK UP AND RESTORE



New Developments (0-1 years)

- GFS policy on disk first, then on tape
- Crossover Backup across sites

Legacy

- Backup to Tape in AA & BUC
- Backup to Disk in AA & BUC

Strategy (2-4 years)

- N/A
- N/A

To Watch

- DataDomain
- Backupless solutions.
- Backup as a Service (Cloud)

Our new data centre communication links provide new capabilities so that we can back up across sites while improving bandwidth and throughput. Backup audits must be performed on a regular basis as well as frequent restores in a random way. This will help to avoid duplicating unnecessary data, improve backup windows but also what is most important, the efficiency and effectiveness of our backup policies.

The use of new functionalities like improved compression and deduplication (at source or post-process) can help to achieve a less data and faster backups. The number of copies and its retention will define the level of data protection. The GFS (Grandfather-Father-Son) policy can be supported and complemented by a five level backup tiering as follows:

1. Tier 1: Online data (running on the different environments)
2. Tier 2: Replicated data.
3. Tier 3: Backup to disk.
4. Tier 4: Backup to Tape.
5. Tier 5: Off-site backup (Disk copy on different site first and then, if not, tapes off shoring. Or both).

13 Networking

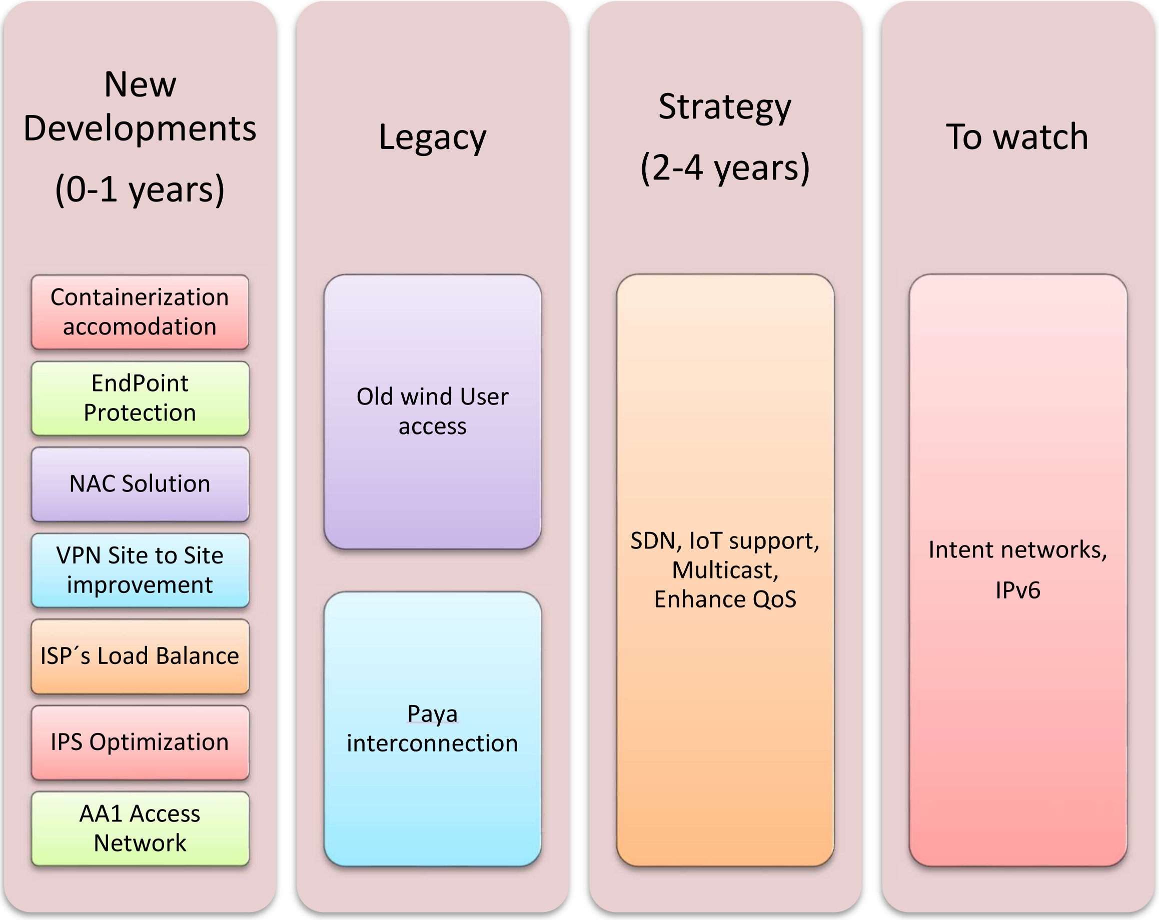
13.1 NETWORK FOUNDATION

The computer networking model is based on the TCP/IP family of protocols. The IP version is IPv4. The data links layer is Ethernet. with 1Gbps for users endpoints and 1Gbps/10Gbps for servers, depending on the bandwidth demand of each servers.

Backbone links bandwidth is 20 Gbps but scalable to 80 Gbps.

Loops are not allowed in the network topology. HA at the link level must be provided by Port aggregation techniques. Spanning tree protocol will not block ports so no convergence time is needed.

Network devices providing connectivity to critical services for the Office will be deployed in high availability to avoid single point of failures.



New Developments (0-1 years)

- Containerization accomodation
- EndPoint Protection
- NAC Solution
- VPN Site to Site improvement
- ISP´s Load Balance
- IPS Optimization
- AA1 Access Network

Legacy

- Old wind User access
- Paya interconnection

Strategy (2-4 years)

- SDN, IoT support, Multicast, Enhance QoS

To watch

- Intent networks, IPv6

13.2 NETWORK LAYERS ARCHITECTURE

EUIPO network model follows the popular Cisco Enterprise Composite Model. This model clearly defines the organization network as a set of different layers according to their purpose.

The Cisco Enterprise Architecture attempts to describe how all the network components integrate and work together. It includes Campus, Data Center, Branch, WAN, and Teleworker components.

The Campus Architecture component is basically the same as in the Composite model. It includes routing and switching integrated with technologies such as IP telephony and is designed for high availability with redundant links and devices. It integrates security features and provides QoS to ensure application performance. It is flexible enough to add advanced technologies such as VPNs, tunnels, and authentication management.

The core module is the portion of the network that routes and switches traffic as fast as possible from one network to another. This is simply the core layer in the hierarchical network model.

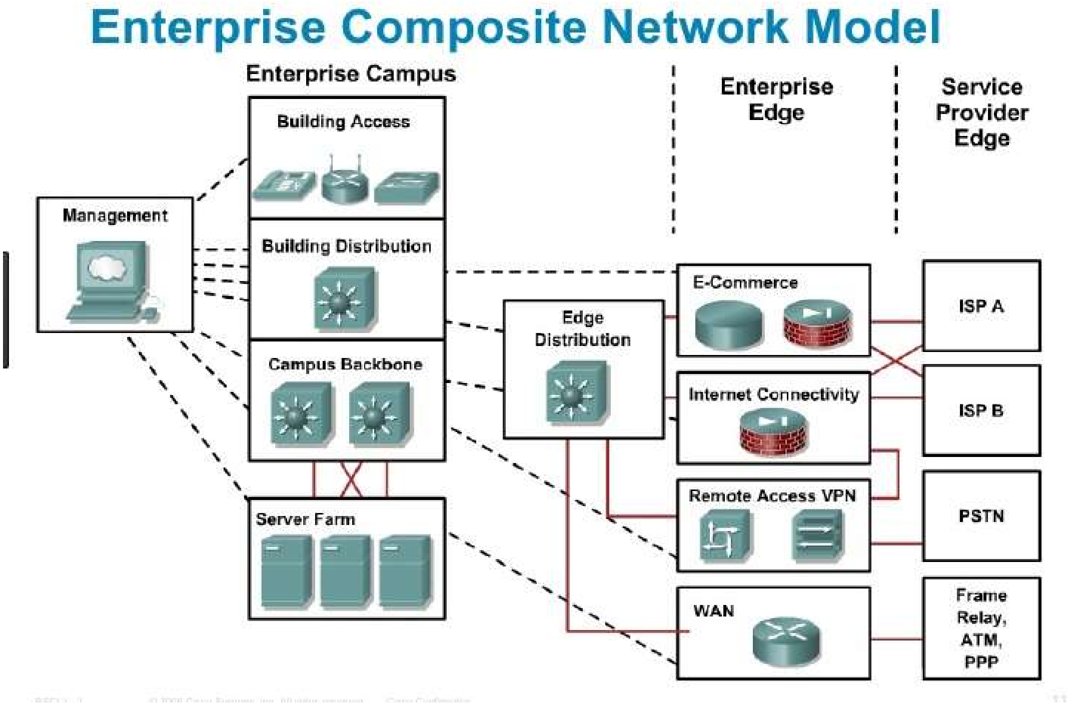
The management module allows for the secure management of all devices and hosts within the enterprise. Within this module, logging and reporting information flows from the devices to the management hosts, while content, configurations, and new software flows to the devices from the management hosts.

The Data Center component provides a centralized, scalable architecture that enables virtualization, server and application access, load balancing, and user services. Redundant data centers might be used to provide backup and business continuity.

The Branch Architecture extends enterprise services to remote offices. Network monitoring and management is centralized. Branch networks include access to enterprise–level services such as converged voice and video, security, and application WAN optimization. Resiliency is obtained through backup local call processing, VPNs, redundant WAN links, and application content caching.

The WAN component provides data, voice, and video content to enterprise users any time and any place. QoS, SLAs, and encryption ensure a high–quality secure delivery of resources. It uses IPsec or MPLS VPNs over Layer 2 or Layer 3 WANs, with either a hub–and–spoke or mesh topology.

Teleworker Architecture describes how voice and data are delivered securely to remote small or home office users. It leverages a standard broadband connection, combined with VPN and identity–based access. An IP phone can also be used.



13.3 ROUTING PROTOCOLS

OSPF v4 is the default routing protocol for the intranet. Static routes are allowed in specific zones. Static routes should be redistributed into OSPF and NHRP techniques are a must when using static routes.

BGP4 is the routing protocol used to interact with the ISPs

13.4 ZONE SEGMENTATION

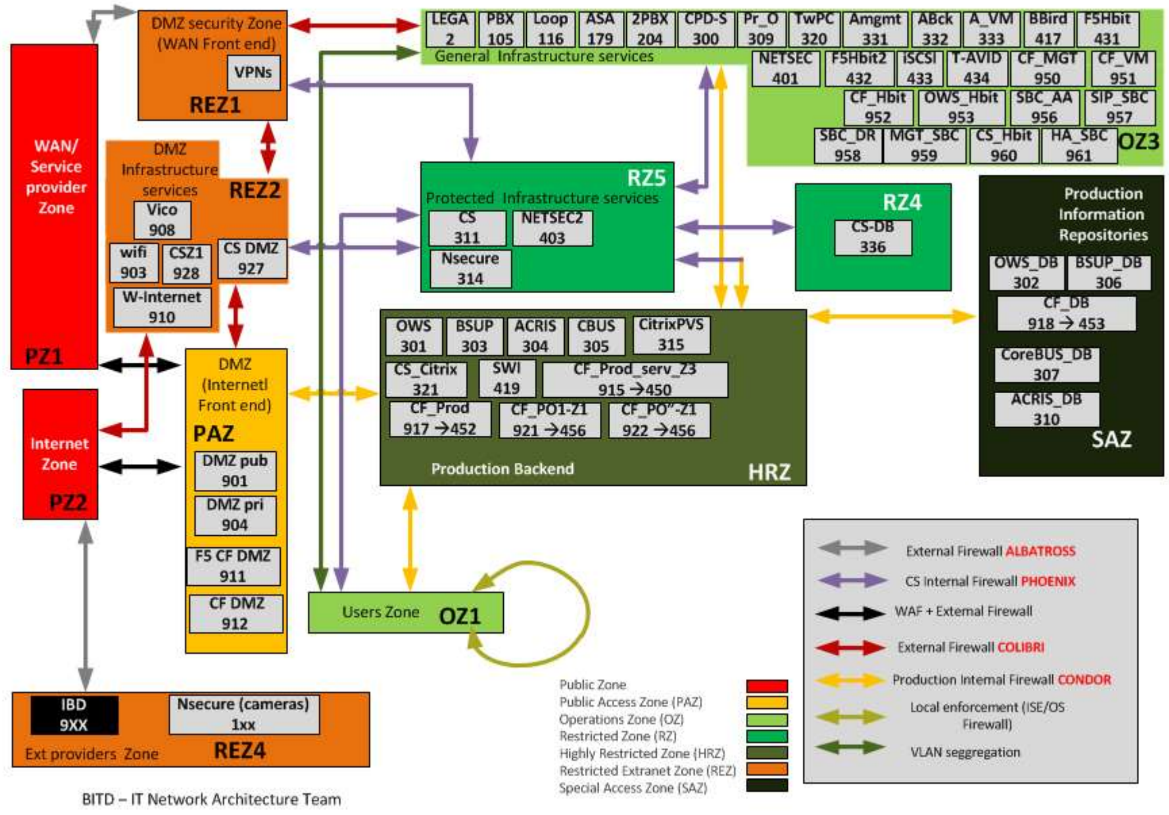
Network will be segmented[1] following the network segregation plan taking place at the time of this writing.

For the development of new applications, a multitier application with separation of the tiers in different segment of the network will be applied for security purposes.

The network segregation plan defines new zones for allocating services depending on their criticality level. Regarding the development of new applications and its placement within the different zones, the philosophy of 3 different zones remains but new naming convention changes applies as well as the security enforcement is enhanced by the use of different firewalls for different environments.

Network segregation presents the following zones and defines the connectivity between them in the following way for production environment:

[1] Current segmentation process is ongoing.



Focusing on the applications, in the DMZ the Load Balancer (F5 for EUIPO deployment or Apache for NOs deployment) will be balancing the load and acting as a Web Application Firewall (WAF) for protecting applications. It will contain also the static content of applications.

A DMZ Security zone contains any authentication or authorisation mechanism (CAS, AD, etc…) used by FO applications.

The HRZ zone will contain the dynamic content and the Business Logic of the applications. Integrations will be performed by ESB with a load balancer acting also as WAF for protecting services invocations.

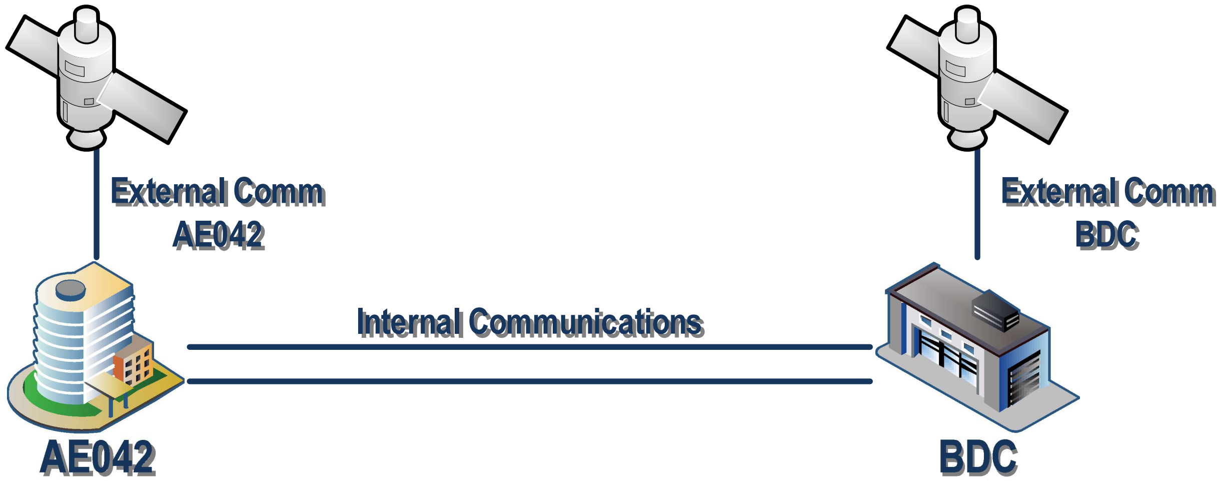
Any data and file repository will be hosted in the SAZ zone, in order to guarantee consistency and integrity. Search engines will be hosted in the HRZ. A Load Balancer will be available in case functionality by Data or Application Server will not be provided.

The OZ3 zone will contain all infrastructure support services like Backup, monitoring, etc.

14 Datacentres

The EUIPO has two datacentres (DCs) which are closely interconnected. The first DC is located at Agua Amarga new wing (AE42 S2). The second one is hosted by Banco Sabadell. Both DCs are 3 around Kms from each other.

Business Continuity and High Availability is being guaranteed by redundant power and cooling equipment. Two different telecom companies provide up to 2 x four 10GB Ethernet interconnections and 2 x two 8Gbps FC interconnections. The two DCs connect each other through the DWDM equipment located in the telecom rooms (AA) or racks (BS).



At the time we design and implement any application or system, although two physical locations, only one logical DC will be considered as we have an Extended Datacentre. Therefore, we shall design active-active solutions so that we can provide the same service from different sites without disruption and for services that do not require active-active we'll define solutions where the switch or failover and back are processed with as much automation as possible.

Based on the Recovery Time Objective (RTO) defined in the Business Impact Analysis (BIA), the following availability mode shall be designed:

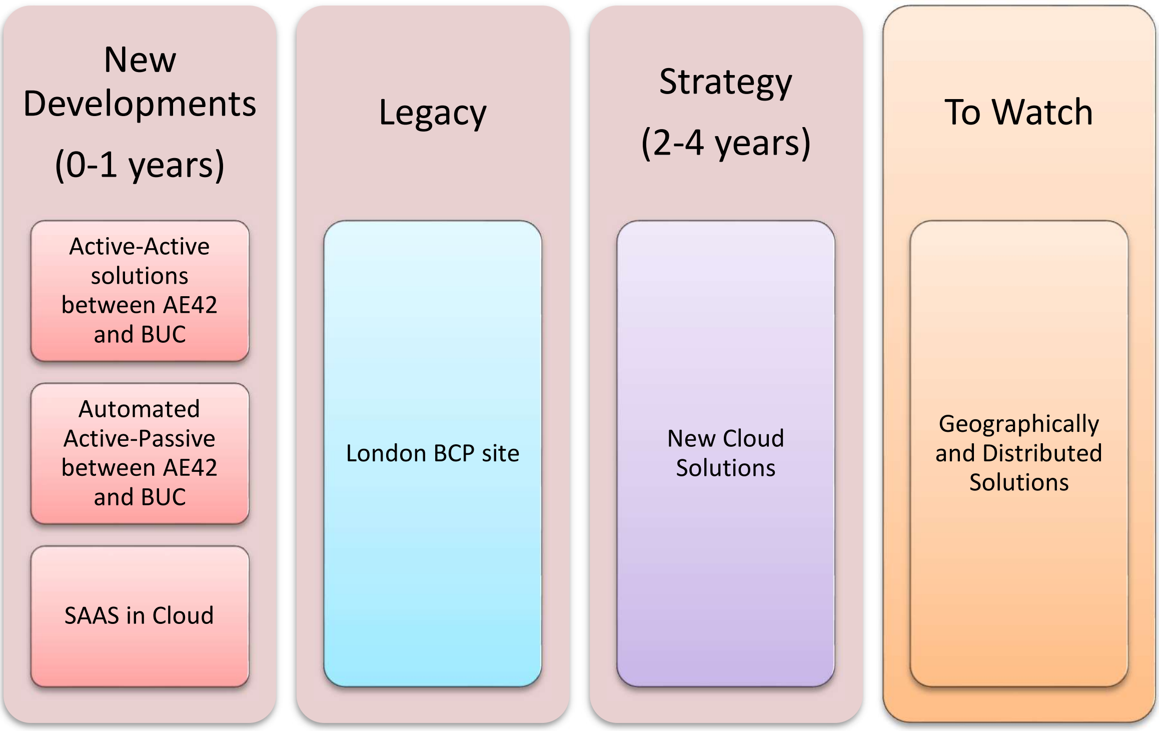
- The services to be restored in less than 24 hours should run in active-active high availability (HA) in the 2 data centres (DC).
- Standby mode is acceptable for the service to be restored in less than 48 hours, but the preference goes to active-active.
- All the services to be restored in less than 1 week are installed at least in standby in the back-up centre.
- The services to be restored in 1 week and more have to be installed in passive mode in the second DC.

All the production data has to be replicated in the second DC, the replication mode shall be selected based on the RTO (a service with a short RTO shall have data accessible in active-active between the 2 DC) and the Recovery Point Objective (RPO) that is also specified in the BIA.

As a result, replication between sites will performed at the application level first. If this is not possible, then it will be performed at the database or operating system layer. If none of these is available then we'll replicate at the storage level through SAN mechanisms.

To achieve this objective, our latency must remain below 1 ms. between both DCs. Exceptions will be evaluated by the IT architecture team.

In case of natural disaster destroying both DCs, the BCP DC at London shall be activated. Currently this DC hosts a standalone website and standalone version of TM and RCD eFiling. The new version of the BIA that is in acceptance process at the time of writing this Reference Architecture is requesting shorter RTO. This will require an extension of the BCP site.


New Developments (0-1 years)
Active-Active solutions between AE42 and BUC
Automated Active-Passive between AE42 and BUC
SAAS in Cloud
Legacy
London BCP site
Strategy (2-4 years)
New Cloud Solutions
To Watch
Geographically and Distributed Solutions

15 Others

15.1 TELEPHONY

CISCO VoIP Switchboard is used.

16 SAP

SAP here is understood as an ecosystem. This chapter describes the Reference Architecture for the implementation of a generic application developed on SAP enterprise reference platform. In EUIPO Reference Architecture, although from the logical point of view some solutions are part of more generic frameworks such as BI or the presentation layer, SAP products are presented as a whole.

Following the SAP macro functional area, this section depicts the selected reference architecture from a logical point of view, pointing out a detailed level for each functional area.

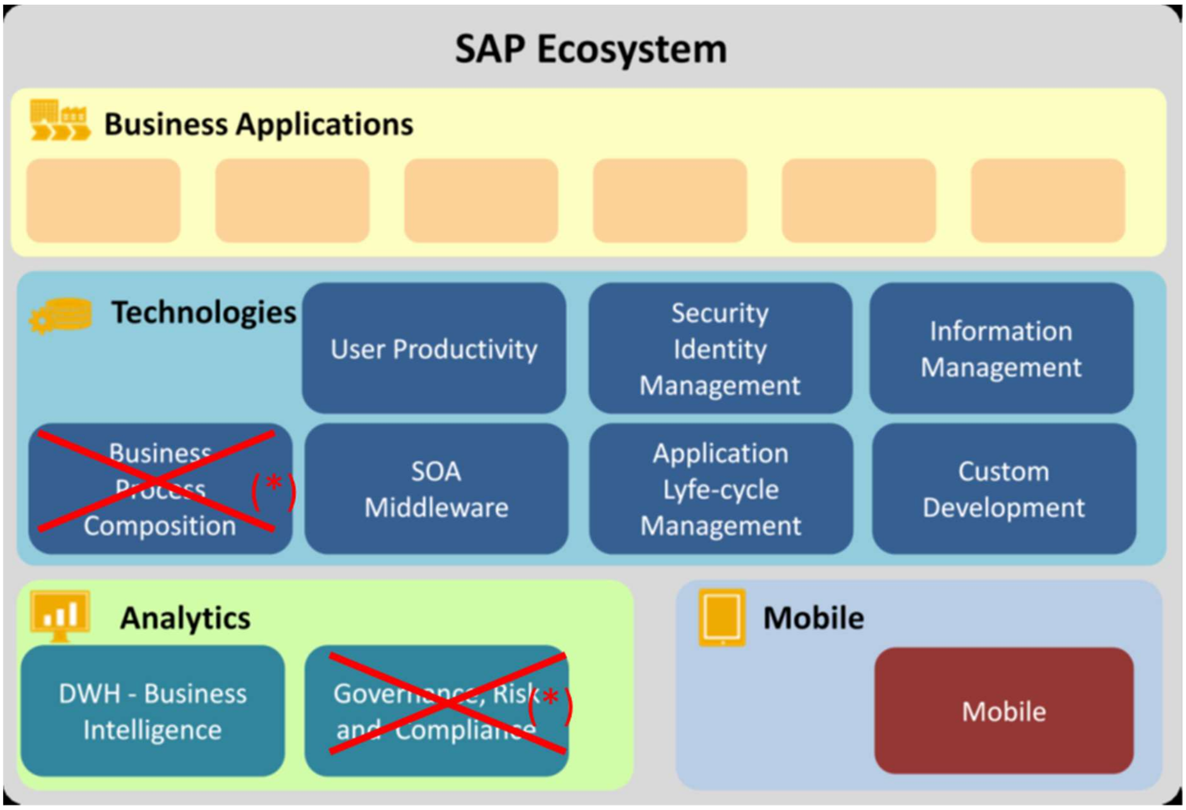

SAP Ecosystem
Business Applications
Technologies
User Productivity
Security Identity Management
Information Management
~~Business Process Composition~~ (*)
SOA Middleware
Application Lyfe-cycle Management
Custom Development
Analytics
DWH - Business Intelligence
~~Governance, Risk and Compliance~~ (*)
Mobile
Mobile

Figure 1 SAP organization

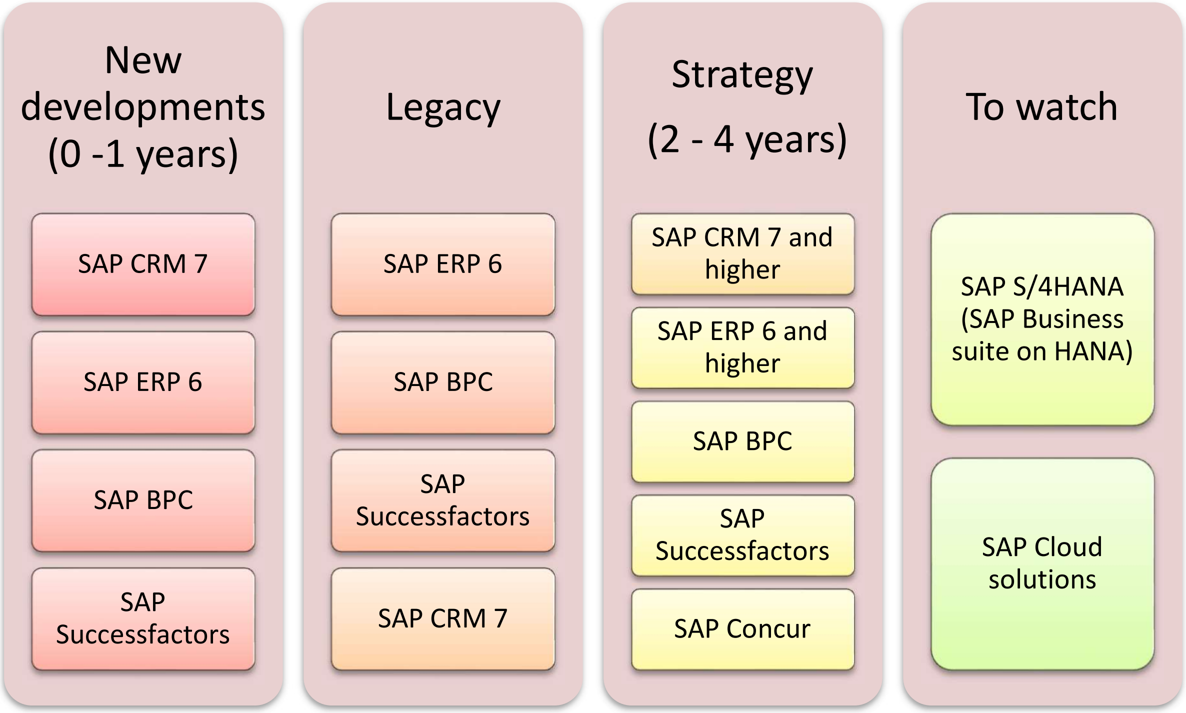
(*) Not used in EUIPO

16.1 BUSINESS APPLICATION AREA

The “core” of the SAP Ecosystem is constituted of a set of business applications, based on a Service Oriented Architecture (SOA), that are able to support end-to-end Company processes like:

- SAP ERP (Enterprise Resource Planning)
- SAP CRM (Customer Relationship Management)
- SAP Contact Center (Business Communications Management)
- SAP Succesfactors (Human Capital Management)
- SAP BPC (Business Planning and Consolidation)

It is important to underline that this document mentions such Business Applications only for reference, because it is strictly focused on the technologies and solutions used or that might be used within the organization.

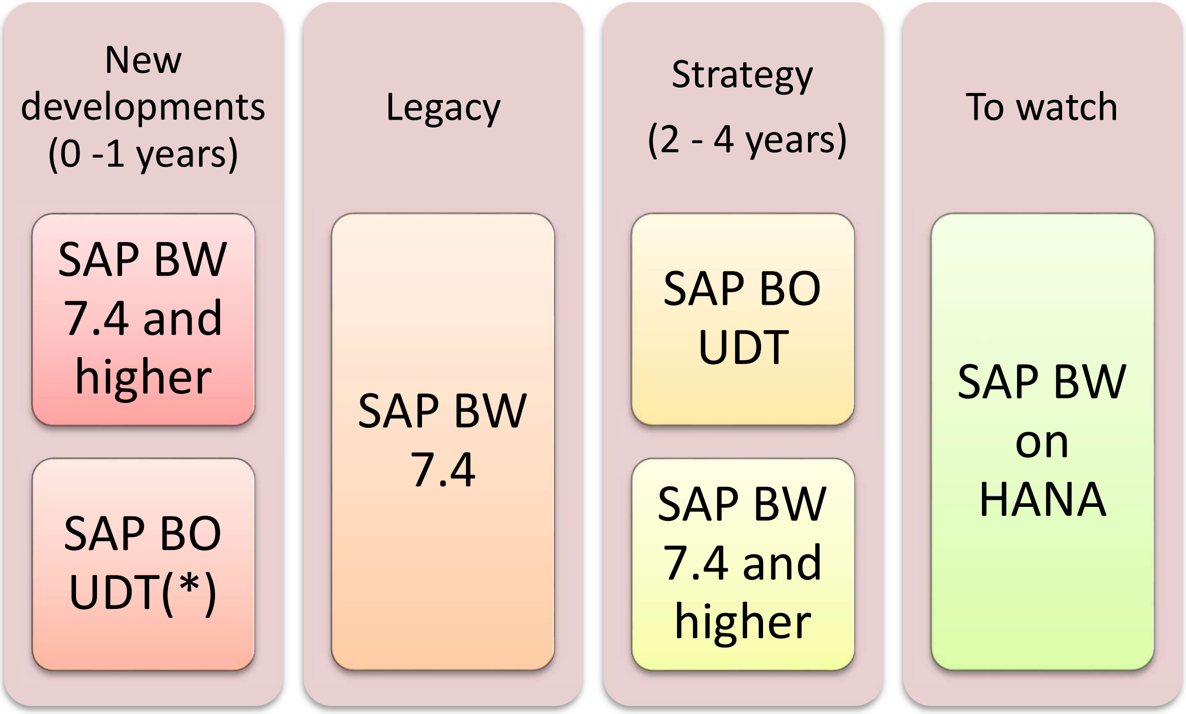


New developments (0 -1 years)	Legacy	Strategy (2 - 4 years)	To watch
SAP CRM 7	SAP ERP 6	SAP CRM 7 and higher	SAP S/4HANA (SAP Business suite on HANA)
SAP ERP 6	SAP BPC	SAP ERP 6 and higher	SAP Cloud solutions
SAP BPC	SAP Successfactors	SAP BPC	
SAP Successfactors	SAP CRM 7	SAP Successfactors	
		SAP Concur	

16.2 DWH - BUSINESS INTELLIGENCE

The Business Intelligence block relates to business intelligence functionality that can help users to make effective, informed decisions based on structured data and analysis. With these solutions, users will have the possibility to access, format, analyse, navigate, and share information across the whole organization.

The Data Warehousing Process (DWH) is the way that data distributed in the operational databases (which is non homogeneous, duplicated, inconsistent by nature and often not easily accessible) is extracted, rationalized, in some cases enriched with data coming from outside EUIPO, transformed and made available in an environment that is separated from the original operational data store: the data warehouse.

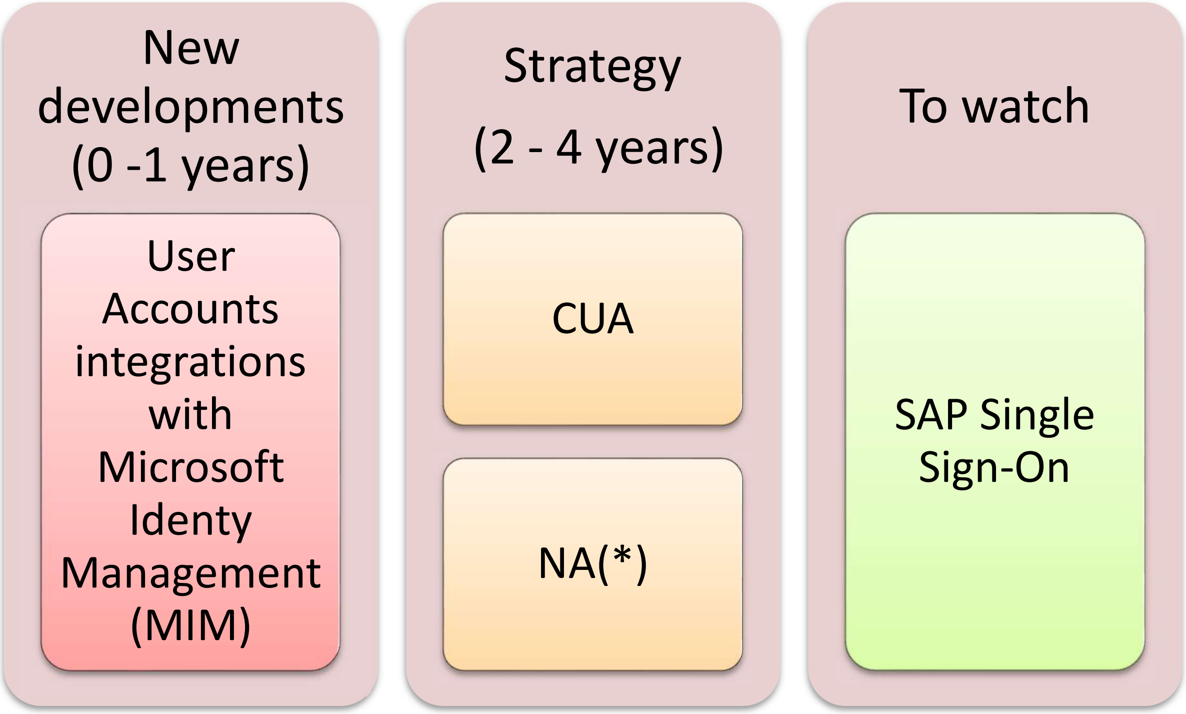


New developments (0 -1 years)	Legacy	Strategy (2 - 4 years)	To watch
SAP BW 7.4 and higher SAP BO UDT(*)	SAP BW 7.4	SAP BO UDT SAP BW 7.4 and higher	SAP BW on HANA

(*) SAP BO Universe designer tool is the BO functionality for data analysis and processing.

16.3 SECURITY AND IDENTITY MANAGEMENT

With the increasing use of distributed systems and the Internet, for managing business data, the demands on security are also on the rise. When using a distributed system, we need to be sure that the data and processes support our business needs without allowing unauthorized access to critical information.



New developments (0 -1 years)

User Accounts integrations with Microsoft Identy Management (MIM)

Strategy (2 - 4 years)

CUA

NA(*)

To watch

SAP Single Sign-On

(*) SAP ecosystem can be included in a global or SAP specific SSO architecture. This will be defined in next framework deliverables.

16.4 USER PRODUCTIVITY

The User Productivity block relates to a set of technologies that help users and groups to improve their productivity through enhanced collaboration, optimized knowledge management and intuitive search in business objects as well as unstructured content.

User Productivity is about simplified access to structured and unstructured information, enrichment of applications and access channels with standardized services, and enablement of user interface development, in both the Java and the ABAP stack, through the use of integrated design and modelling tools.

It also has to include personalized access to mission-critical applications and data accomplished, using: portals, desktop clients and mobile interfaces. For all that, the use of flexible UI technology could enable final and technical users, to build their own state-of-the-art applications.

The different clients will have the ability to utilize the User Productivity services and repositories and provide the end user, feature and application consistency through the multiple channels. This reusing leads to an overall IT benefit by reduced complexity and cost.

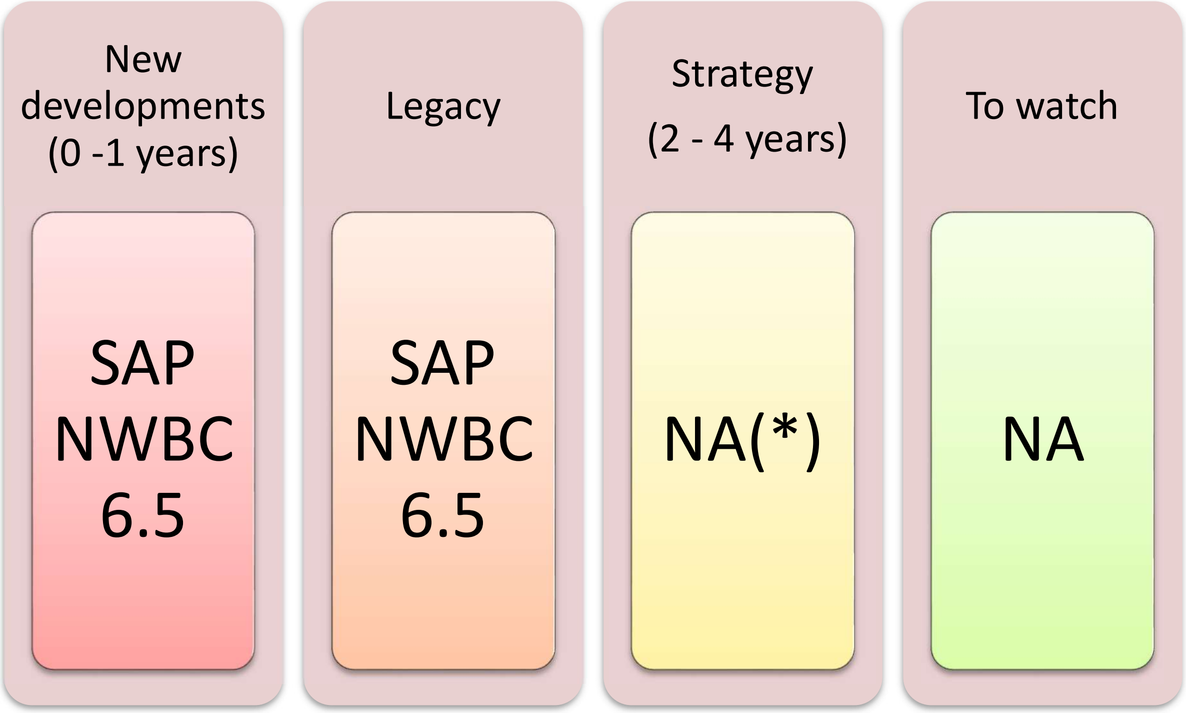
16.4.1 Solutions

New developments (0 -1 years)	Legacy	Strategy (2 - 4 years)	To watch
Sap Interactive Forms by Adobe	SAP EP 7.0	Sap Interactive Forms by Adobe	SAP HANA Cloud Portal
SAP BCM 7.7	SAP BCM 7	SAP BCM 7 and higher versions	SAP Enterprise Portal 7.4
SAP Fiori 2.0	Sap Interactive Forms by Adobe	SAP Fiori 2.0 and higher versions	

16.4.2 Reporting

New developments (0 -1 years)	Legacy	Strategy (2 - 4 years)	To watch
SAP Business Objects BI platform 4.2	SAP Business Objects BI platform 4.2	SAP Lumira 2.0 and higher versions	NA
SAP Business Objects Crystal Reports 4.2	SAP Business Objects Crystal Reports 4.2	SAP Business Objects BI platform 4.2 and higher versions	
SAP Business Objects Web Intelligence 4.2	SAP Business Objects Web Intelligence 4.2	SAP BusinessObjects Crystal Reports 4.2 and higher versions	
SAP Business Objects Dashboard 4.2	SAP Business Objects Dashboard 4.2	SAP BusinessObjects Web Intelligence 4.2 and higher versions	
		SAP BusinessObjects Dashboard 4.2 and higher versions	

16.4.3 Heavy clients



New developments (0 -1 years)	Legacy	Strategy (2 - 4 years)	To watch
SAP NWBC 6.5	SAP NWBC 6.5	NA(*)	NA

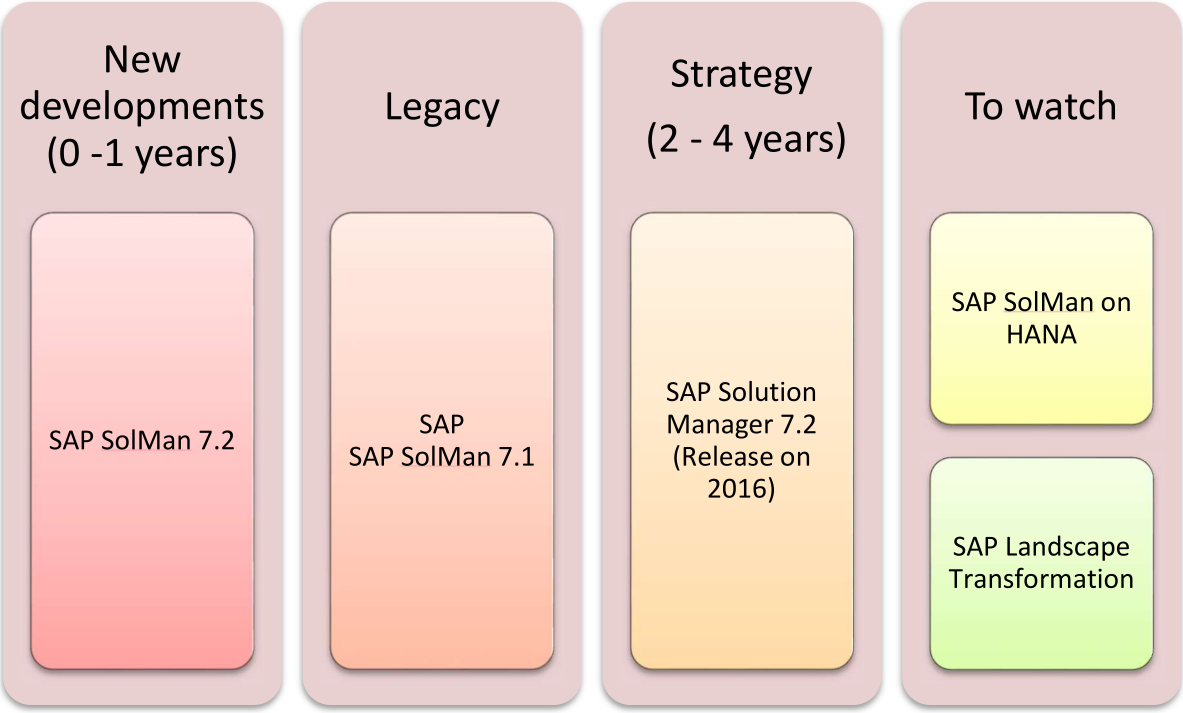
(*) We will keep using heavy clients for technical users and define a strategy for business users.

16.5 APPLICATION LIFE-CYCLE MANAGEMENT

The Application Life-cycle Management block relates to processes, tools, services, and an organizational model to manage SAP throughout the complete application life cycle.

The results of the different phases of the application life cycle can be leveraged by other phases due to the integration provided by SAP Solution Manager helping to implement solutions.

The Framework might include directives for the deployment, transport management, operations and infrastructure related activities.



New developments (0 -1 years)

SAP SolMan 7.2

Legacy

SAP
SAP SolMan 7.1

Strategy

(2 - 4 years)

SAP Solution Manager 7.2 (Release on 2016)

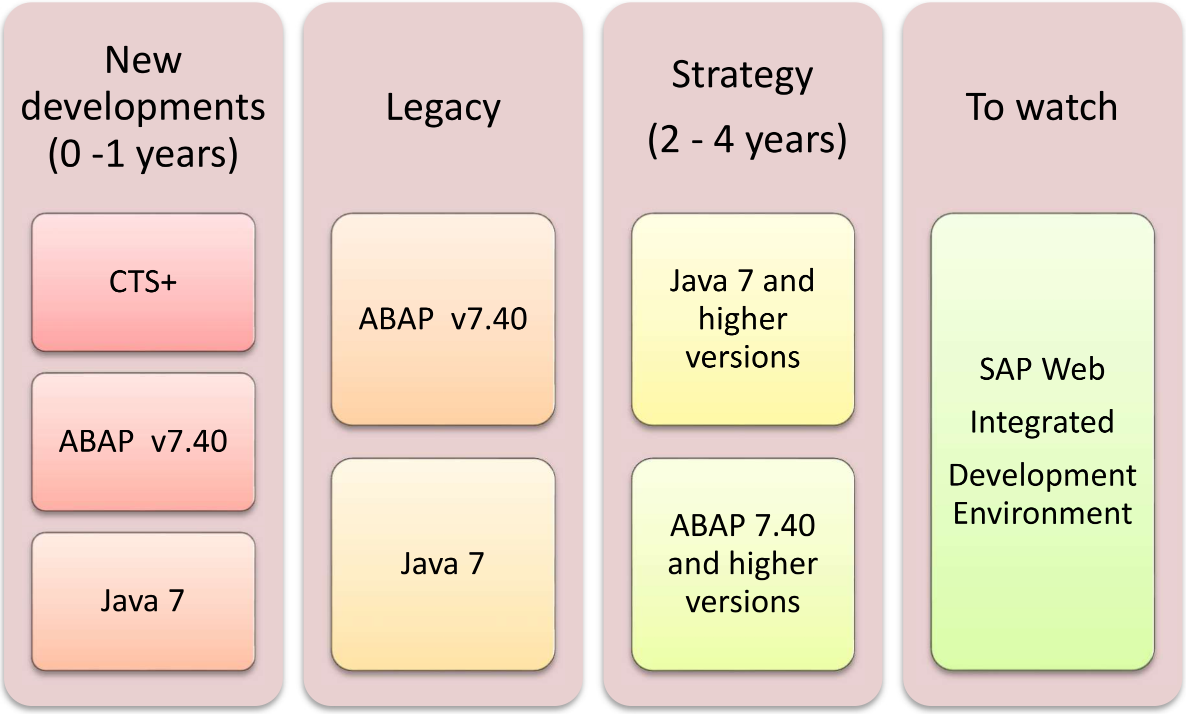
To watch

SAP SolMan on HANA

SAP Landscape Transformation

16.6 CUSTOM DEVELOPMENT

The Custom Development block relates to specific procedures and guidelines for SAP Business Process extension / enhancement and the creation of custom applications using either the ABAP or Java programming language.



New developments (0 -1 years)

CTS+

ABAP v7.40

Java 7

Legacy

ABAP v7.40

Java 7

Strategy (2 - 4 years)

Java 7 and higher versions

ABAP 7.40 and higher versions

To watch

SAP Web Integrated Development Environment

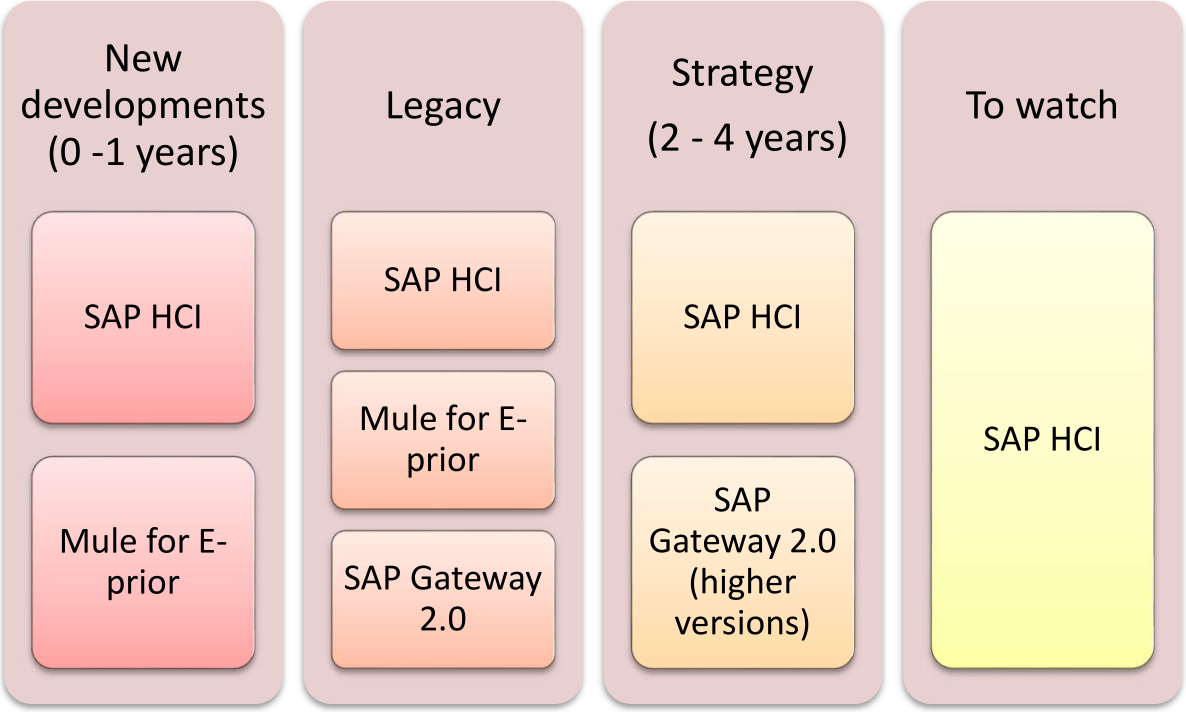
16.7 SOA MIDDLEWARE

The SOA Middleware block relates to a set of disciplines and services oriented to enable the use (standards-based) of Enterprise Service Oriented architecture (SOA) within a SAP project, based on the approach and technologies included in the SAP suite (standard Enterprise Services under the Enterprise Service Repository).

From a logical point of view, SAP SOA middleware consists of:

- An enterprise services repository and registry.
- An enterprise services bus (ESB).
- SOA management tools.

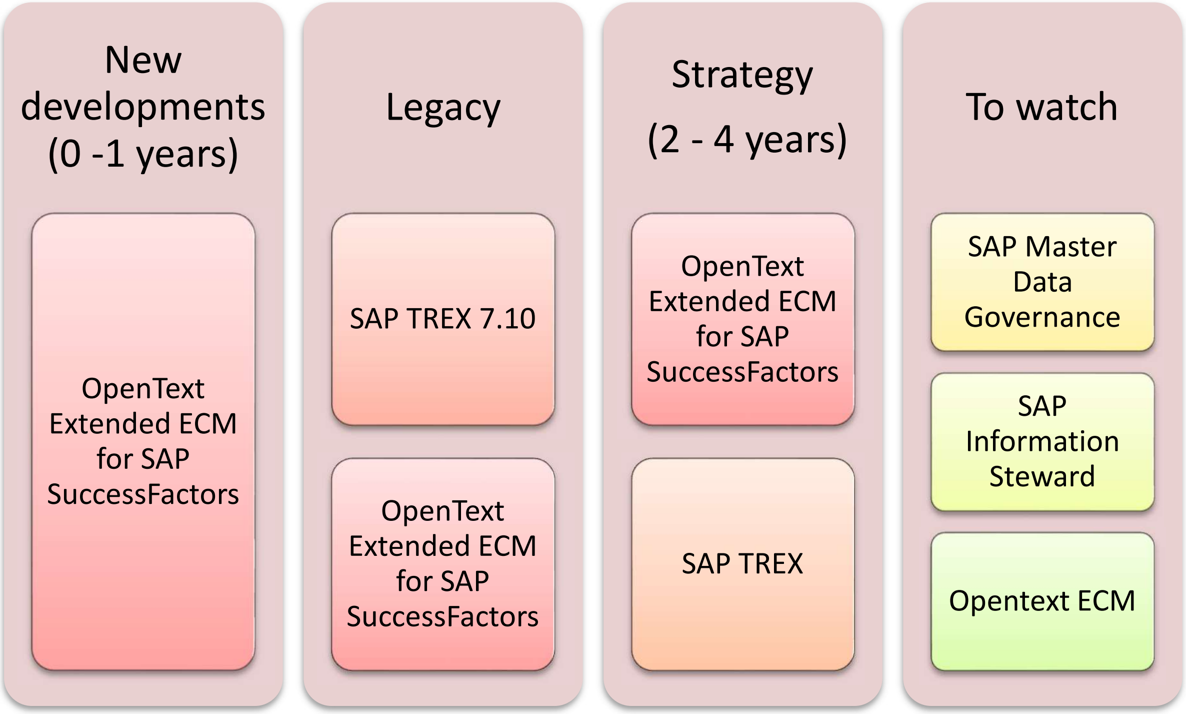
The main objective is to accelerate business integration through an open and standard based platform. EUIPO is using SAP Hana Cloud Integration (HCI) for all integrations involving SAP cloud systems. The integration with Commission E-Prior platform is done via Mule as in that time HCI was not part of the EUIPO tool set and while being Mule still a reference architecture tool a migration to HCI is not a need as there are not additional values identified for this migration.



16.8 INFORMATION MANAGEMENT

Within the information management tag we include tools for master data management, ETLs, data quality as well as enterprise content management tools and standards.

Data Services is an ETL with data cleansing capabilities, **SAP Information Steward(IS)** is a tool with a console for data quality, it also allows you to create changes and import them in the **SAP DS**. **SAP MDG** is a tool for master data management; it is installed as an add-on on an ERP. **SAP ECM** is a tool for EIM. SAP works fine with most of enterprise content management platforms



New developments (0 -1 years)

- OpenText Extended ECM for SAP SuccessFactors

Legacy

- SAP TREX 7.10
- OpenText Extended ECM for SAP SuccessFactors

Strategy (2 - 4 years)

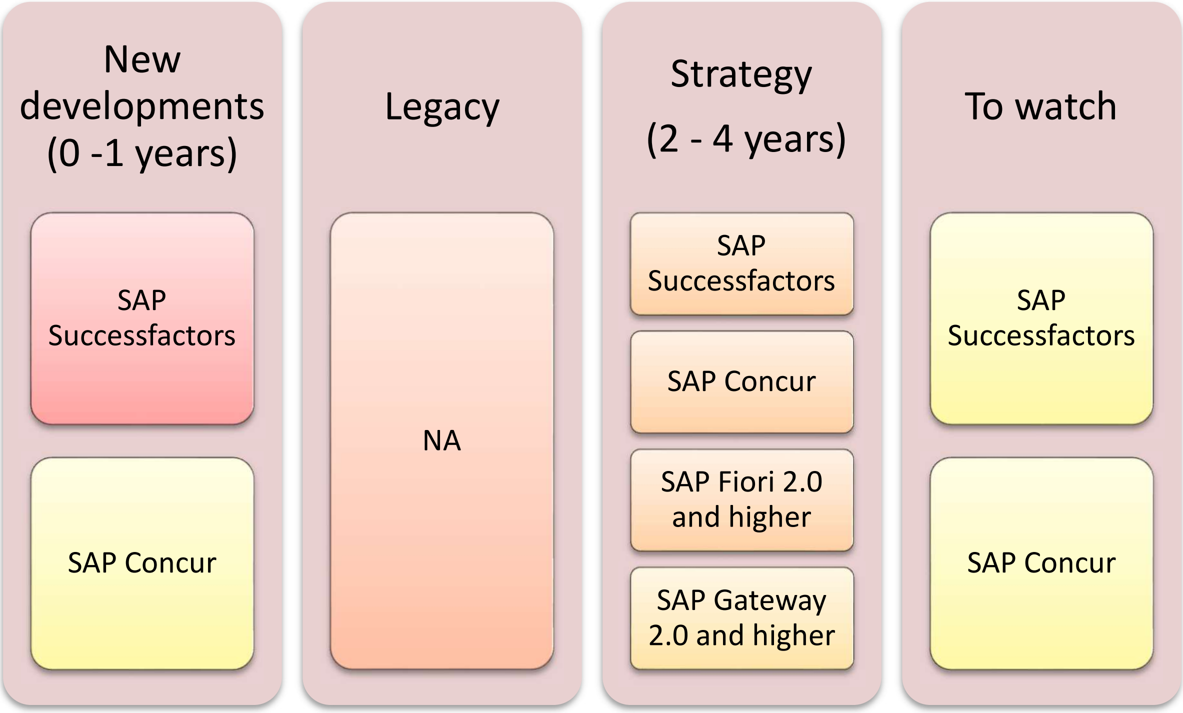
- OpenText Extended ECM for SAP SuccessFactors
- SAP TREX

To watch

- SAP Master Data Governance
- SAP Information Steward
- Opentext ECM

16.9 MOBILE

Solutions based on SAP platform that will have to provide services through the use of mobile devices. The SAP mobile solution has to be aligned with the general Mobile reference architecture.



New developments (0 -1 years)

- SAP Successfactors
- SAP Concur

Legacy

- NA

Strategy (2 - 4 years)

- SAP Successfactors
- SAP Concur
- SAP Fiori 2.0 and higher
- SAP Gateway 2.0 and higher

To watch

- SAP Successfactors
- SAP Concur